Configuring IPX Services

BayRS Version 13.00
Site Manager Software Version 7.00

BCC Version 4.05

Part No. 303531-A Rev. 00
October 1998

Bay Networks *Where Information Flows.™*

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. October 1998.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FRE, LN, Optivity, PPX, Quick2Config, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, BayRS, BaySecure, BayStack, BayStream, BCC, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, FN, IP AutoLearn, PathMan, RouterMan, SN, SPEX, Switch Node, System 5000, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin xvii
Text Conventions xviii
Acronyms xix
Bay Networks Technical Publications xxi
How to Get Help xxii

Chapter 1
IPX Concepts

About the IPX Protocol 1-2
Network-Layer Services 1-3
Supported LAN Circuits, WAN Circuits, and Frame Formats 1-3
Handling Packets Associated with Upper-Layer Protocols 1-5
IPX Host ID Numbers 1-6
Multipath Routing and Load Sharing 1-7
Multipath Routing 1-7
Load Redistribution and Rerouting 1-10
Multipath Route Precedence/Priority 1-10
Multipath Configurations 1-10
Multiline Circuits 1-10
Types of IPX Configurations 1-12
IPX Ping Support 1-13
Role of Bay Networks Routers in a Client/Server Connection 1-13
Example: Client/Server Connection via Bay Networks Router 1-15
For More Information About IPX 1-17

Chapter 2
Starting IPX Services Using the BCC

Starting IPX 2-2
Step 1: Configuring a Physical Interface 2-2
Step 2: Configuring an IPX Interface 2-2
Starting IPXWAN Services 2-3
Step 1: Configuring a Physical Interface 2-3
Step 2: Configuring a WAN Protocol 2-4
Step 3: Configuring an IPXWAN Interface 2-4
Starting RIP 2-5
Starting SAP 2-5

Chapter 3
Starting IPX Services Using Site Manager

Starting IPX 3-2
Starting IPXWAN Services 3-3
Starting RIP and SAP Services 3-4
Deleting RIP and SAP from an IPX Interface 3-5
Customizing RIP and SAP 3-5

Chapter 4
Customizing IPX for LAN Media

Specifying Multiple Interfaces per Circuit 4-1
IPX Host ID Numbers 4-5
Setting an IPX Host ID Number on a Token Ring Circuit 4-6
Configuring a Multiple-Host Router 4-7
Configuring a Single-Host Router 4-9
Token Ring MAC Address Selection 4-11
Customizing IPX 4-11

Chapter 5
Customizing IPX for WAN Media

IPX over WAN Media 5-2
Using IPXCP and IPXWAN 5-2
Running IPXWAN over PPP 5-3
Running IPXWAN over Frame Relay Permanent Virtual Circuits 5-3
Negotiating an IPXWAN Connection 5-3

Identifying a Circuit 5-4
Entering an IPX Host ID Number for IPX 5-4
Disabling and Reenabling IPXWAN for an Interface 5-7
Assigning a Primary Network Number 5-8
Entering a Router Name 5-9
Indicating the Protocol Negotiated for an Interface 5-10
Sample IPXCP and IPXWAN Configurations 5-12
IPXCP Link Negotiation 5-13
IPXWAN Link Negotiation 5-13
IPXWAN and IPXCP Link Configurations 5-14
Configuration 1 (IPXWAN with IPXCP on Both Interfaces) 5-15
Configuration Guidelines -- Configuration 1 5-15
Configuration 2 (IPXWAN on Both Interfaces) 5-15
Configuration Guidelines -- Configuration 2 5-15
Configuration 3 (IPXCP on Both Interfaces) 5-16
Configuration Guidelines -- Configuration 3 5-16
Configuration 4 (Interfaces Do Not Share IPXCP or IPXWAN) 5-16
Customizing IPX 5-16

Chapter 6
Customizing IPX

Customizing IPX Global Parameters 6-2
Setting the Maximum Number of Paths 6-2
Filtering Log Messages 6-3
Specifying the Maximum Number of Equal-Cost Paths 6-5
Specifying the Maximum Number of Destinations 6-6
Entering the Maximum Number of Services 6-8
Specifying the Aging Time for RIP and SAP Information 6-10
Specifying the Aging Pending Frequency 6-11
Enabling IPX Default Routing 6-13
Selecting the GNS Response Mode 6-14
Specifying the Table Fill Notify Value 6-16
Specifying the Size of the Network Table 6-16
Specifying the MIB Reply Slot 6-16
Specifying the Routing Method 6-17
Specifying the Maximum Number of Hops 6-18

Indicating the Number of Next-Hop Hosts 6-19
Customizing an IPX Interface 6-21
Disabling and Reenabling IPX Routing on an Interface 6-21
Entering a Symbolic Name for an Interface 6-22
Assigning a Host Number to an Interface 6-23
Choosing a Frame Encapsulation Type 6-25
Enabling Source Routing for an Interface on a Token Ring Circuit 6-26
Specifying a Broadcast Address 6-29
Specifying a Multicast Address 6-30
Setting the Delay Time 6-32
Specifying Throughput 6-33
Setting the Stabilization Timer Delay 6-34
Setting a Cost for an Interface 6-35
Customizing RIP Parameters 6-38
Disabling and Reenabling RIP 6-40
Enabling RIP Listen and Supply Functions 6-41
Determining the Pace of RIP Packets 6-42
Configuring RIP Timers 6-43
Adjusting the RIP Packet Size 6-46
Enabling Multicast Transmission of RIP Packets 6-47
Configuring Split Horizon 6-49
Fully Meshed Networks 6-50
Non-Fully Meshed Networks 6-50
Updating Routers About a New or Failed Route 6-53
Advertising Default Routes in RIP Packets 6-54
Accepting Default Route Information 6-55
Customizing SAP Parameters 6-56
NetWare Directory Services (NDS) and SAP 6-56
SAP and the NetWare Bindery (NetWare 3.*x* and Earlier) 6-56
Disabling and Reenabling SAP 6-57
Configuring SAP Timers 6-58
Configuring a Default Route for SAP 6-60
Enabling SAP Listen and Supply Functions 6-61
Determining the Pace of SAP Packets 6-63
Adjusting the SAP Packet Size 6-64

Responding to SAP GNS Requests 6-65
Using a Multicast Address 6-66
Saving the Full Service Name in SAP Packets 6-67
Transmitting and Receiving SAP Updates over the Same Interface 6-68
Updating Routers About a New or Failed Service 6-70
Using Static Services 6-71
Setting the Update Interval and Disabling Immediate Updates 6-71
Adding a Static Service 6-74
Enabling Static Services 6-76
Specifying the Network Address of a Service 6-77
Specifying the Address of the Host That Provides a Service 6-78
Specifying the Socket Address of a Service 6-79
Specifying the Hop Count 6-80
Customizing NetBIOS Static Routing 6-81
Adding a NetBIOS Static Route 6-83
Disabling and Reenabling the Static Route Record in the NetBIOS Routing Table 6-85
Directing a NetBIOS Packet Using Nonstandard Static Routing 6-86
Directing a NetBIOS Packet Using Standard Static Routing 6-88
Configuring NetBIOS Broadcast Filters 6-88
Configuring an Adjacent Host for an Interface 6-92
Creating an Adjacent Host 6-93
Disabling and Reenabling the Adjacent Host 6-94
Entering the ID of the Adjacent Host 6-95
Entering a WAN Address 6-96
Creating a Frame Relay SVC to an Adjacent Host 6-98
Dial Services for IPX 6-101
Using Dial-on-Demand Service 6-102
Using Static Routing with Dial-on-Demand 6-103
Tips for Using Dial-on-Demand with IPX 6-104
Enabling Local IPX Watchdog Acknowledgment 6-104
Configuring Dial-Optimized Routing for IPX 6-106
Getting Optimum Performance Using IPX Dial-Optimized Routing 6-107
Default IPX Dial-Optimized Routing Filters 6-108
Configuring RIP and SAP Broadcast Timers 6-109

Using Static Routes 6-110
Configuring a Static Route 6-113
Changing the Target Network Address 6-114
Entering the Hop Count 6-115
Setting the Timer Ticks 6-117
Using RIP Route Filters 6-118
Using SAP Filters 6-119
Using SAP Filters at the Server Level 6-123
Using SAP Filters at the Network Level 6-124
Using Wildcards and Pattern Matching with SAP Filters 6-127
Using Wildcards with SAP Filters 6-127
Using Pattern Matching with SAP Filters 6-129
Example of Using SAP Filters 6-133
Configuring Service Name Filters 6-134
Enabling an IPX Service Name Filter 6-134
Specifying the Target Server Name 6-136
Specifying the Target Service Type 6-138
Setting the Filter Priority 6-139
Applying Filters to Inbound or Outbound Packets 6-140
Specifying the Protocol 6-141
Specifying How to Process SAP Advertisements 6-143
Specifying a Cost 6-144
Deleting IPX from the Router 6-147

Appendix A
BCC IPX Parameters

IPX Global Parameters A-2
IPXWAN Parameters A-6
Static NetBIOS Route Parameters A-9
IPX Interface Parameters A-10
IPX Adjacent Host Parameters A-13
RIP Parameters A-14
Route Filter Parameters A-16
SAP Parameters A-18
Server Name Filter Parameters A-21
Server Network Filter Parameters A-23

Static Route Parameters A-25
Static Service Parameters A-26

Appendix B
Site Manager IPX Parameters

IPX Configuration Parameters B-2
IPXWAN Configuration Parameters B-7
IPX Global Parameters B-9
IPX Advanced Global Parameters B-13
IPX Interface Parameters B-22
IPX Change Circuit Parameters B-30
IPX RIP Circuit Parameters B-35
IPX SAP Circuit Parameters B-41
IPX NetBIOS Static Route Configuration Parameters B-46
IPX NetBIOS Static Route Parameters B-48
Adjacent Host Configuration Parameters B-50
IPX Adjacent Hosts Parameters B-53
IPX Static Route Configuration Parameters B-56
IPX Static Route Parameter Descriptions B-59
IPX Static Service Configuration Parameters B-61
IPX Static Service Parameters B-64
Route Filter Configuration Parameters B-67
IPX Route Filter Parameters B-69
Service Network Filter Configuration Parameters B-74
IPX Service Network Filter Parameters B-77
IPX Service Name Filter Configuration Parameters B-82
IPX Service Name Filter Parameters B-84

Appendix C
BCC show Commands for IPX

show ipx summary C-2
show ipx adjacent-hosts C-2
show ipx forwards C-3
show ipx hosts C-3
show ipx interfaces C-4
show ipx rips C-5

show ipx route-filters C-6
show ipx routes C-7
show ipx saps C-8
show ipx server-name-filters C-8
show ipx server-network-filters C-9
show ipx services C-10
show ipx static-netbios-routes C-11
show ipx static-routes C-12
show ipx static-services C-12
show ipx stats C-13

Appendix D
Common Service Types and Identifiers

Appendix E
Sample IPX Configuration

Configuration Particulars E-2
Router 1 ..... E-2
Router 2 ..... E-3

Index

Figures

Figure 1-1. Frames Received at a Logical Interface 1-6
Figure 1-2. Frames Issued from a Logical Interface 1-7
Figure 1-3. IPX Multipath Routing 1-8
Figure 1-4. IPX Multipath Routing -- Equal Least-Cost Routes 1-9
Figure 1-5. Sample IPX Network 1-16
Figure 4-1. Multiple IPX Interfaces per Physical Circuit 4-3
Figure 4-2. Frames Received at a Logical Interface 4-5
Figure 4-3. Frames Sent from a Logical Interface 4-6
Figure 5-1. IPXCP and IPXWAN Configurations 5-12
Figure 6-1. IPX Routers Source Routing across a Token Ring Network 6-27
Figure 6-2. IPX Interface Cost 6-36
Figure 6-3. IPX Configurable RIP Timers 6-44
Figure 6-4. Split Horizon Enabled in a Fully Meshed Network 6-50
Figure 6-5. Split Horizon Disabled in a Non-Fully Meshed Network 6-51
Figure 6-6. Static Service Network Configuration 6-72
Figure 6-7. IPX SAP Filters Prohibiting SAP Broadcasts 6-73
Figure 6-8. NetBIOS Static Routes 6-83
Figure 6-9. NetBIOS Packet Filtering 6-90
Figure 6-10. NetBIOS Packet Flow 6-91
Figure 6-11. NetBIOS Broadcast Filtering 6-92
Figure 6-12. Dial-on-Demand Service 6-103
Figure 6-13. IPX Static Routes 6-112
Figure 6-14. SAP Outbound Filtering 6-122
Figure B-1. IPX Configuration Window B-3
Figure B-2. IPXWAN Configuration Window B-7
Figure B-3. Edit IPX Global Parameters Window B-9
Figure B-4. IPX Advanced Global Parameters Window B-13
Figure B-5. IPX Interfaces Window B-22
Figure B-6. IPX Change Circuit Window B-31

Figure B-7. IPX RIP Circuit Window B-35
Figure B-8. IPX SAP Circuit Window B-41
Figure B-9. IPX NetBIOS Static Route Configuration Window B-46
Figure B-10. IPX NetBIOS Static Routes Window B-48
Figure B-11. IPX Adjacent Host Configuration Window B-50
Figure B-12. IPX Adjacent Hosts Window B-53
Figure B-13. IPX Static Route Configuration Window B-56
Figure B-14. IPX Static Routes Window B-59
Figure B-15. IPX Static Services Configuration Window B-61
Figure B-16. IPX Static Services Window B-64
Figure B-17. IPX Route Filter Configuration Window B-67
Figure B-18. IPX Route Filters Window B-69
Figure B-19. IPX Service Network Filter Configuration Window B-74
Figure B-20. IPX Service Network Filters Window B-77
Figure B-21. IPX Service Name Filter Configuration Window B-82
Figure B-22. IPX Service Name Filters Window B-84
Figure E-1. Sample IPX Configuration E-2

Tables

Table 1-1. LAN Circuit and Frame Support for IPX Interfaces 1-4
Table 1-2. WAN Circuit and Frame Support for IPX Interfaces 1-4
Table 5-1. Configuration Table for IPX over WAN Media 5-14
Table 6-1. Characters in SAP Pattern-Matching Filters 6-129
Table 6-2. Concatenation Rules and Operators 6-131
Table A-1. IPX Global Parameters A-2
Table A-2. IPXWAN Parameters A-6
Table A-3. Static NetBIOS Route Parameters A-9
Table A-4. IPX Interface Parameters A-10
Table A-5. IPX Adjacent Host Parameters A-13
Table A-6. RIP Parameters A-14
Table A-7. Route Filter Parameters A-16
Table A-8. SAP Parameters A-18
Table A-9. Server Name Filter Parameters A-21
Table A-10. Server Network Filter Parameters A-23
Table A-11. Static Route Parameters A-25
Table A-12. Static Service Parameters A-26
Table D-1. Service Types and Identifiers D-1

Preface

This guide describes the Internetworking Packet Exchange (IPX) protocol and what you do to start and customize IPX services on a Bay Networks® router.

You can use the Bay Command Console (BCC™) or Site Manager to configure IPX on a router. In this guide, you will find instructions for using both the BCC and Site Manager.

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Bay Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** <*ip_address*>, you enter: **ping 192.32.10.12**
bold text	Indicates text that you need to enter and command names and options. Example: Enter **show ip** {**alerts** | **routes**} Example: Use the **dinfo** command.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you must enter either: **show ip alerts** or **show ip routes**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is: **ethernet/2/1** [<*parameter*> <*value*>] . . ., you enter **ethernet/2/1** and as many parameter-value pairs as needed.

italic text	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.
`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

ARE	all-routes explorer (frame)
ATM	asynchronous transfer mode
AUI	attachment unit interface
BootP	Bootstrap Protocol
BRI	Basic Rate Interface
CCITT	International Telegraph and Telephone Consultative Committee (now ITU-T)
CSMA/CD	carrier sense multiple access with collision detection
DLCI	data link connection identifier
DLCMI	Data Link Control Management Interface

GNS	get nearest server
GUI	graphical user interface
HDLC	high-level data link control
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IPXCP	Internetwork Packet Exchange Control Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector (formerly CCITT)
LAN	local area network
LSAP	link service access point
MAC	media access control
MAU	media access unit
MDI-X	media-dependent interface with crossover
MIB	management information base
MTU	maximum transmission unit
NBMA	nonbroadcast multi-access
NCP	Network Control Protocol
NDS	NetWare Directory Services
NIC	network interface card
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First (protocol)
PDN	Public Data Network
PNN	primary network number
PPP	Point-to-Point Protocol
PROM	programmable read-only memory
RIF	routing information field
RIP	Routing Information Protocol

SAP	Service Advertisement Protocol
SMDS	Switched Multimegabit Data Service
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPX	Sequenced Packet Exchange
SRE	specific route explorer
STP	shielded twisted pair
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TPE	twisted pair Ethernet
WAN	wide area network
XNS	Xerox Network System

Bay Networks Technical Publications

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the Bay Networks product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase Bay Networks documentation sets, CDs, and selected technical publications through the Bay Networks Collateral Catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

How to Get Help

For product assistance, support contracts, or information about educational services, go to the following URL:

http://www.baynetworks.com/corporate/contacts/

Or telephone the Bay Networks Technical Solutions Center at:

800-2LANWAN

Chapter 1
IPX Concepts

This chapter describes IPX concepts you need to know before you begin configuring an interface on a circuit.

Topic	Page
About the IPX Protocol	1-2
Network-Layer Services	1-3
Supported LAN Circuits, WAN Circuits, and Frame Formats	1-3
Handling Packets Associated with Upper-Layer Protocols	1-5
IPX Host ID Numbers	1-6
Multipath Routing and Load Sharing	1-7
Types of IPX Configurations	1-12
IPX Ping Support	1-13
For More Information About IPX	1-17

About the IPX Protocol

The Internetwork Packet Exchange (IPX) protocol is the Novell, Inc. adaptation of the Xerox Network System (XNS) protocol.

IPX has the following characteristics:

- It is a *connectionless datagram* delivery protocol. *Connectionless* means that it does not need a channel established for packet delivery. A *datagram* is a unit of data that contains all the addressing information required for it to be delivered to its destination. The path or route that one datagram follows to reach a destination is independent of the path or route that another datagram may follow to reach the same destination.
- It does not guarantee the delivery of packets. Upper-layer protocols assume the responsibility for reliability. The upper-layer protocols that IPX uses are SPX and NCP.
- It uses the Internet Data Packet (IDP) format.

IPX is the network layer routing protocol used in the NetWare environment. The primary tasks of IPX are addressing, routing, and switching information packets from one location to another on a network. The network interface card (NIC) in a client provides network node addressing. IPX defines the *internetwork* and *intranode* addressing as follows:

- *Network addresses* form the basis of the IPX internetwork addressing scheme for sending packets between network segments. Every network segment of an internetwork is assigned a unique network address that routers use to forward packets to their final destinations. A network address in the NetWare environment consists of 8 hexadecimal characters. In the following example, *0x* indicates that this is a hexadecimal number, and *n* is any hexadecimal character.

  0xnnnnnnnn

- *Socket numbers* are the basis for an IPX intranode address, that is, the address of an individual entity within a node. They allow a process (for example, RIP or SAP) to distinguish itself to IPX. To communicate on the network, the process must request a socket number. Any packets that IPX receives addressed to that socket are then passed on to the process within the node.

Network-Layer Services

A Bay Networks router running IPX provides the following network-layer support:

- Dynamic routing of IPX packets
- Multiple IPX interfaces per circuit
- IPX over WAN media
- IPXWAN and IPXCP
- Routing Information Protocol (RIP and Unnumbered RIP)
- Service Advertisment Protocol (SAP)
- Static route support
- Default route support
- Adjacent host support
- Dial-on-demand support

Supported LAN Circuits, WAN Circuits, and Frame Formats

IPX supports various combinations of physical circuits and data link layer frame formats. You can choose the ones that are appropriate for the types of clients and applications on your network.

Table 1-1 lists the types of LAN circuits and frame formats supported by Bay Networks routers running IPX.

Table 1-1. LAN Circuit and Frame Support for IPX Interfaces

Circuit Type	Frame Type (Novell Terminology)	Frame Type (Bay Networks Terminology)
Ethernet	ETHERNET_II ETHERNET_802.2 ETHERNET_802.3 ETHERNET_SNAP	ETHERNET LSAP NOVELL SNAP
Token ring	TOKEN-RING TOKEN-RING_SNAP	LSAP SNAP
FDDI	N/A	LSAP SNAP

Table 1-2 shows the relationships between different WAN circuits,WAN protocols, and frame formats supported by Bay Networks routers running IPX.

Table 1-2. WAN Circuit and Frame Support for IPX Interfaces

Circuit Type	WAN Protocol	Frame Format (Bay Networks Terminology)
Synchronous -V.35 -RS-232/V.24 -RS-422/423 -X.21 -T1/Fractional T1 -E1/Fractional E1	 ATM Frame relay PPP SMDS X.25 Point-to-Point X.25 PDN Bay Networks Point-to-Point	 SNAP SNAP PPP SNAP ETHERNET RFC 1356 ETHERNET
HSSI	ATM Frame relay PPP SMDS Bay Networks Point-to-Point	SNAP SNAP PPP SNAP ETHERNET
ISDN	PPP	PPP

You can use these tables when you select an encapsulation method. For more information about the encapsulation method, see “Specifying Multiple Interfaces per Circuit” on page 4-1.

Handling Packets Associated with Upper-Layer Protocols

The router encapsulates any packets associated with Novell’s upper-layer protocols within the data field of an IPX packet. The structure of a packet, as well as the source and destination socket numbers contained in that packet, identify the protocol type associated with that packet, for example, the Service Advertisement Protocol (SAP) and the Routing Information Protocol (RIP). The upper-layer services are:

- Sequenced Packet Exchange (SPX)
- Network Control Protocol (NCP)

Bay Networks router software lets you select the basis on which an IPX router makes its routing decisions: that is, on the number of *ticks* or the number of *hops* required to reach a given destination network. The IPX routing software also provides the following services over LAN and WAN media:

- Multipath routing and load sharing
- Split horizon capability
- NetBIOS all-networks-broadcast packets (type 20 packets)
- Source routing and end-station support
- IPX ping capability

IPX Host ID Numbers

On Bay Networks routers, the IPX host ID number maps to a physical data link layer address (on a specific circuit or physical interface). An IPX logical interface can listen at this address and capture frames transmitted by nodes compatible with IPX on the local data link.

Figure 1-1 illustrates this concept in a Bay Networks router that has two IPX logical interfaces, each one configured on a different physical circuit.

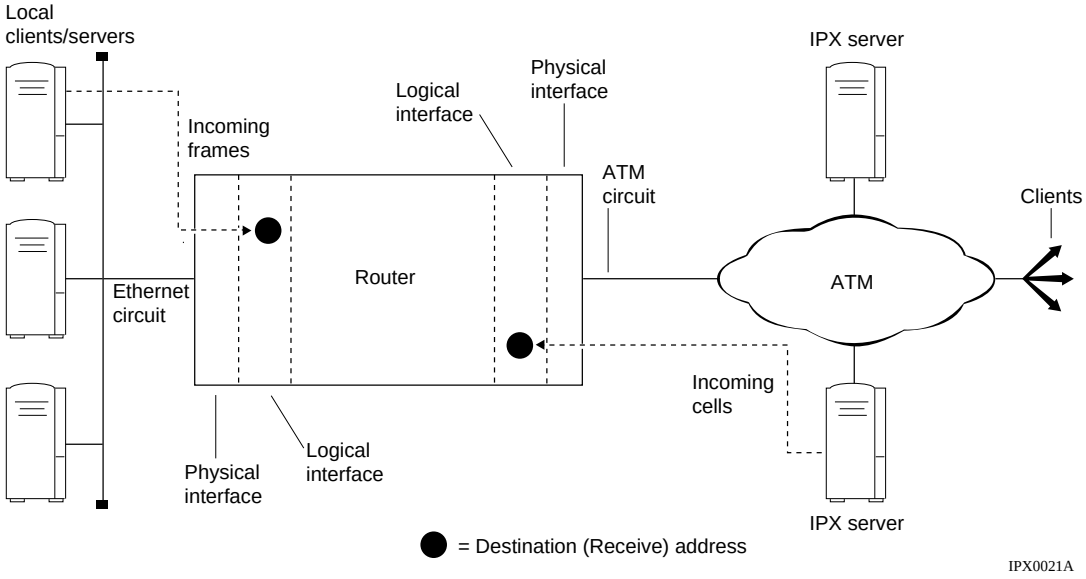

Figure 1-1. Frames Received at a Logical Interface

Figure 1-2 illustrates this concept in a Bay Networks router configured with two IPX logical interfaces, each one on a different physical circuit type.

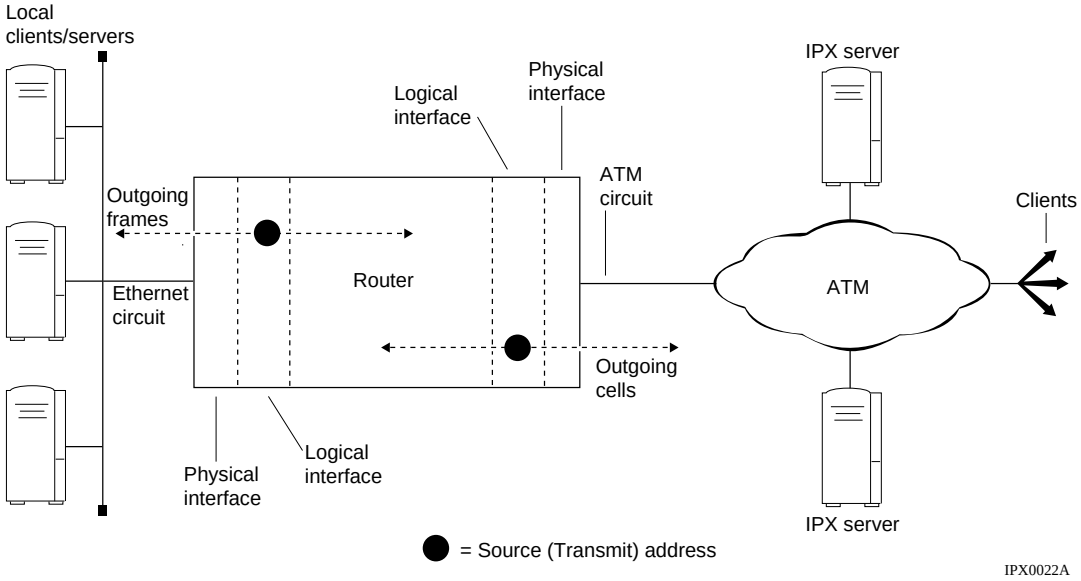

Figure 1-2. Frames Issued from a Logical Interface

Multipath Routing and Load Sharing

You can include multiple next-hop destinations as active routes to a destination network. The IPX router can learn about multiple paths using either RIP packets or statically configured routes.

The router can forward packets to the multiple next-hop nodes concurrently by multiplexing frame transmissions over the multiple equal-cost paths in a cyclic sequence. This is referred to as *IPX multipath* or *IPX load sharing*.

Multipath Routing

Multipath routing is a “round-robin” (or cyclic multiplexing) mechanism. When multiple least-cost paths of equal tick delay and hop count exist between IPX source and destination networks, standard RIP operation uses only one of these routes.

The multipath feature takes advantage of these multiple equal-cost routes and distributes the packet load among them, balancing the IPX traffic across these routes and maximizing internetwork performance. When you enable multipath routing, the IPX router diverts individual, consecutive frames destined for the same target network to separate IPX interfaces and their associated physical circuits (Figure 1-3).

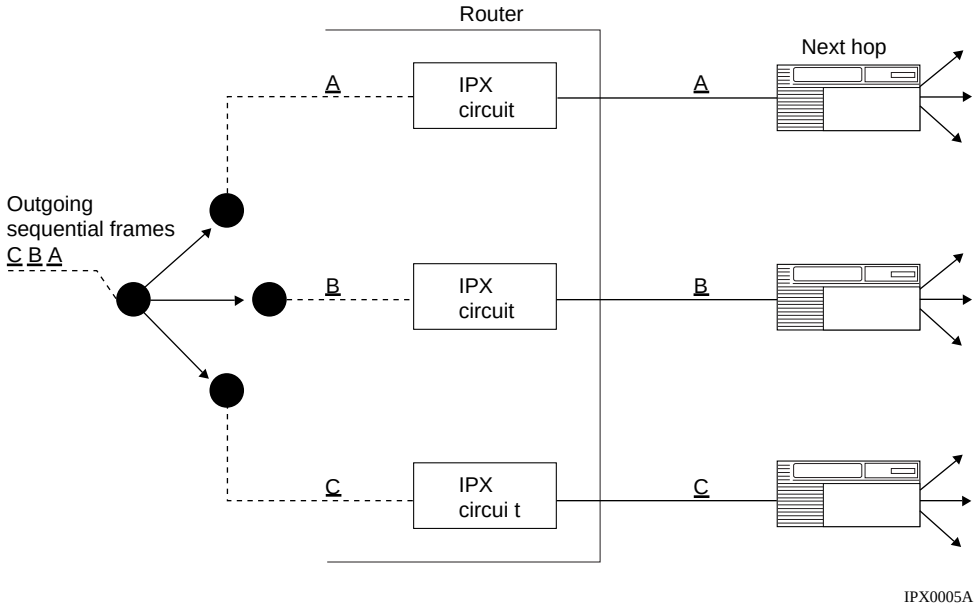

Figure 1-3. IPX Multipath Routing

Because the IPX interfaces have duplex functionality, the router can also use multipath to collect frames received from separate IPX interfaces. The router operates this cyclic mechanism at a bandwidth significantly greater than a single IPX interface and its supporting physical circuit can support. The result is that IPX frames flow over multiple parallel LAN or WAN routes concurrently, in effect, aggregating the bandwidth supported by the parallel routes. Each line shares $1/n^{th}$ of the total load (*n* is the number of equal-cost parallel routes or paths to the destination network).

By default, the maximum number of paths is set to 1. When you specify the maximum number of paths, set the value to the highest number of paths, in the range of 1 to 1,023, that exist from the router to any destination network, regardless of cost. Any setting greater than 1 engages the multipath mechanism. Figure 1-4 is an example of equal, least-cost, parallel routes used in IPX multipath routing.

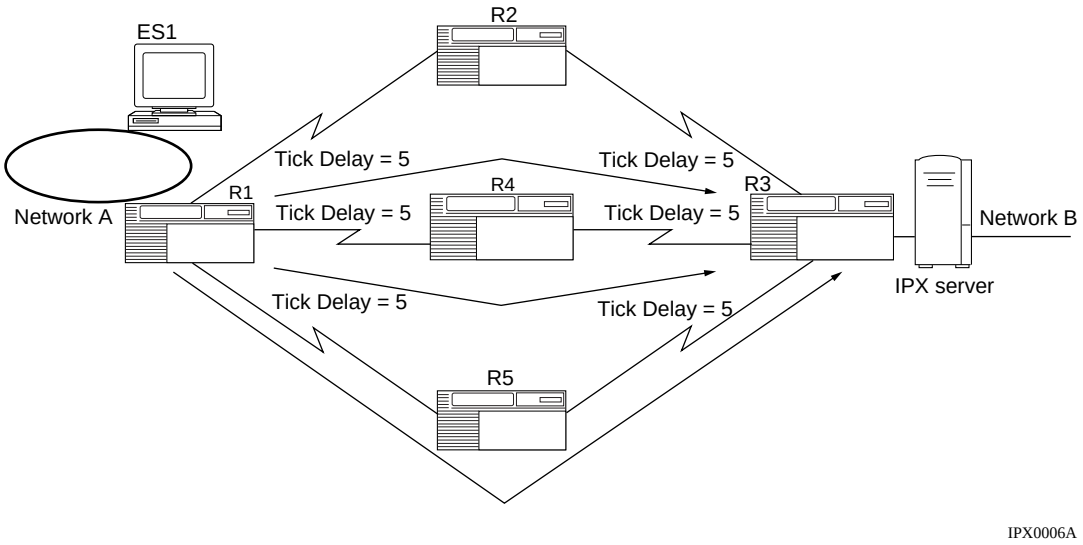

Figure 1-4. IPX Multipath Routing -- Equal Least-Cost Routes

Because of the round-robin algorithm, IPX packets that belong to the same data stream may require resequencing at their final destination. Therefore, higher-layer protocols such as SPX must be used on both source and destination IPX routers to provide packet resequencing. To derive maximum benefit from this feature, the source and destination nodes should support burst-mode operation.

Load Redistribution and Rerouting

If a router with multipath enabled detects a failure, it temporarily redistributes the IPX traffic among the remaining active original least-cost routes. When the router learns (through RIP packets) of the existence of an alternative least-cost route, or when the failed route recovers, IPX multipath resumes its original IPX traffic distribution.

Multipath Route Precedence/Priority

The multipath mechanism generally uses the best path first. However, when two equal-cost paths exist, multipath uses the following priority scheme for route selection:

1. **Direct routes (paths to other routers on a segment directly attached to the local router)**
2. **Routes learned via RIP**
3. **Statically configured routes**

Multipath Configurations

You can establish equal-cost multipath routes over LAN or WAN segments to support IPX traffic between routers, and between routers and servers. The slower the interconnecting LAN or WAN links, the more difference using multipath will make in client/server throughput.

Multiline Circuits

The multiline circuits feature allows a single circuit to be composed of up to 16 individual synchronous network data paths. Multiline circuits support provides a level of redundancy not available through conventional single-line circuit configurations. The multiline circuits feature ensures routing circuit availability in the event of a single data path failure.

Equally important, the multiline circuits feature provides increased bandwidth between two sites without the circuit management complexities associated with multiple circuits. After you configure and enable the circuit, the use of multiple data paths to form a single circuit is transparent to both network management and the end-user community.

Multiline circuits provide the following methods for sending traffic over their data paths:

- Address-based data path selection
- Random data path selection

Address-based data path selection determines the path a packet traverses based on its source and destination addresses. After a path is established for a given address pair, subsequent packets follow the same path, ensuring that packets are received in the order in which they are sent. This is essential for protocols that cannot tolerate receiving packets out of order.

Random data path selection determines the path a packet traverses based on a randomly assigned number that corresponds to a particular data path of the multiline circuit. This algorithm avoids congestion by providing even distribution across multiple data paths. Unlike address-based selection, random data path selection does not guarantee the sequence of packets as they are received at their destination. Consequently, random data path selection is intended for use with protocols whose upper layers provide resequencing techniques.

Note: Multiline circuits can be configured using only synchronous interfaces data paths, including HSSI. All data paths must incorporate the same encapsulation method, maximum transmission unit (MTU), and effective bandwidth.

The differences between multiline circuits and IPX multipath are as follows:

- Multiline circuits operate across point-to-point links between two Bay Networks routers; IPX multipath operates across a random topology (both LAN and WAN).
- Multiline is protocol-independent; IPX multipath is IPX-based.
- Multiline circuits require WAN links of equal bandwidth on which to distribute IPX traffic; IPX multipath supports links of varying speeds.
- Multiline circuits do not support the adoption of alternative links when WAN links fail.

Types of IPX Configurations

The basic types of IPX configurations are:

- *Multiple-host router.* This common configuration supports one IPX interface per circuit; each interface has a unique IPX host number. For information about configuring multiple-host routers, see “Configuring a Multiple-Host Router” on page 4-7.
- *Single-host router.* This standard configuration supports one IPX interface per circuit; each interface shares the same global (“boxwide”) IPX host number. For information about configuring a single-host router, see “Configuring a Single-Host Router” on page 4-9.
- *Multiple interfaces per circuit.* This configuration supports as many IPX interfaces per circuit as there are frame encapsulation types for the given circuit type. For information about configuring multiple interfaces per circuit, see “Specifying Multiple Interfaces per Circuit” on page 4-1.
- *Multiple circuits per segment.* This configuration supports either concurrent bridging and IPX routing or IPX multiline.

IPX Ping Support

The Bay Networks Site Manager supports the IPX ping feature, which uses an IPX diagnostic packet to ping NetWare servers to determine the accessibility -- that is, the status, “alive” or “not responding” -- of the following:

- A remote Bay Networks router
- A Novell IPX server (except as noted later)
- A Novell multiprotocol router
- A NetWare client

This feature can be particularly useful in troubleshooting large networks.

Note: In conformance with the Novell specification, a Bay Networks router running IPX will respond to pings from NetWare servers but will not initiate pings to those servers. Instead, the router running IPX will use diagnostic packets to accomplish the ping function.

Using the IPX **ping** command, the router attempts to communicate with another router running IPX, a server, or an IPX client, and determines whether the destination node is functioning and reachable from the source node. The “pinging” Bay Networks router sends an IPX diagnostic packet, called a configuration request; either the “pinged” router running IPX, the server, or the IPX client responds with a configure response packet.

See *Configuring and Managing Routers with Site Manager* for instructions on using the ping feature in IPX.

Role of Bay Networks Routers in a Client/Server Connection

This section describes how Bay Networks routers running IPX provide clients access to servers on an IPX internetwork.

- Router builds SAP and RIP tables

  The Bay Networks router builds its routing and services tables by listening to regularly scheduled SAP and RIP broadcasts from file servers. The broadcasts include the services a server has to offer and routes to a server. If regular SAP or RIP broadcasts from a file server stops, the local router ages out the entry and removes it from its services or route table.

- Client sends get_nearest_service/get_nearest_directory_server SAP request

  A client sends this request to locate a file server. (Refer to the book, *Novell's Guide to NetWare LAN Analysis*, by Laura Chappell and Dan E. Hawkes, for more information on this mechanism.)

- Router decisions

  If the server resides on the same network as the client, the server receives the request and responds. The local router does not respond because its services table indicates that the service is available on the client's network. In this case, client-router communications stop until the client sends the next get_nearest_service SAP request.

  If the server does not reside on the same network, the router responds, because its services table indicates that the service is not available on the client's network. The SAP response sent by the router contains the server name, the internal address (if applicable), the service type, the socket number, and the intervening network count of the nearest device offering the service.

  If the server does not reside on the same network and multiple servers of the same service type are available, the router picks the server that is the fewest ticks away. If two servers are the same number of ticks away, then the router chooses the server that is the lowest number of hops away. If two servers are the same number of ticks and hops away, then the router chooses based on the alphanumeric order of the server names listed in the services table.

- Client's RIP request

  The client then broadcasts a RIP request packet to the local segment. This packet requests the best path to the server's network.

- Router's RIP response

  The router on the same network as the client refers to its route table and sends a RIP response to the client. The RIP response identifies the network on which the client resides. The RIP response also contains the server's internal network address and the intervening hop and tick count.

- Client's NCP request

  The client sends a Network Core Protocol (NCP) create connection request to the server. The request includes the router's MAC address as the destination address at the data link layer. Within the IPX header, the destination network address is the internal address and the destination node address of the file server. The client forwards the packet to the router.

- Router forwards packet

  The router running IPX forwards the packet to the network identified by the destination network address.

Example: Client/Server Connection via Bay Networks Router

In the example shown in Figure 1-5, client A sends a SAP request to locate a file server. Here is what happens as a result of that request:

1. **Because the server does not reside on LAN A (the same LAN as client A), the Bay Networks IPX router, host 2, sends a SAP response to client A, informing it that the file server, host 3 on token ring 6, is the nearest device offering the requested service.**
2. **Client A then sends a RIP request to determine the best path to host 3.**
3. **The Bay Networks IPX router, host 2, sends a RIP response to client A that includes the server's internal network address and the intervening hop and tick count from host 3 to client A.**
4. **Client A sends an NCP request packet to the Bay Networks IPX router, host 2.**
5. **The router then forwards the packet to host 3.**

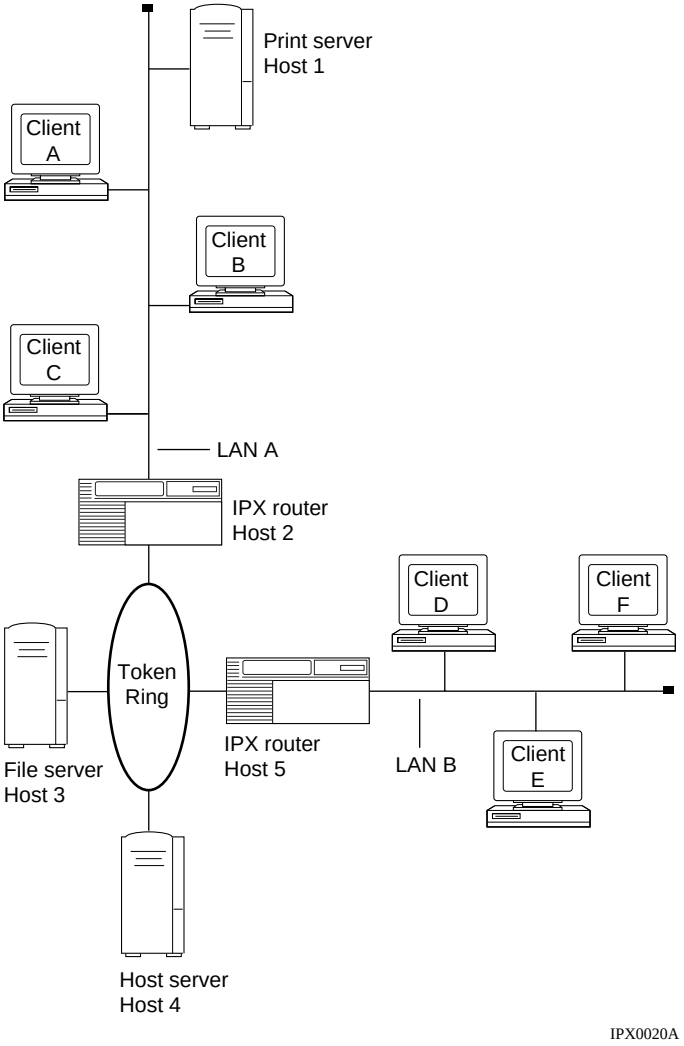

Figure 1-5. Sample IPX Network

For More Information About IPX

The following documents provide technical details about IPX protocol implementation.

RFC 1634: *Novell IPX over Various WAN Media (IPXWAN)*. (Supersedes RFC 1551 and RFC 1362.)

RFC 1552: *The PPP Internetwork Packet Exchange Control Protocol (IPXCP)*.

Novell, Inc. *Advanced NetWare, V.2.0 Internet Packet Exchange Protocol (IPX) with Asynchronous Event Scheduler.* March 19, 1986.

Novell, Inc. *IPX Router Specification.* October 1993.

Chappell, L., and D.E. Hawkes. *Novell's Guide to NetWare LAN Analysis*. Novell Press/Sybex, 1994

Chapter 2
Starting IPX Services Using the BCC

This chapter shows you how to use the Bay Command Console (BCC) to create a basic configuration -- that is, a configuration using all available defaults -- for the IPX services described in this guide.

Topic	Page
Starting IPX	2-2
Starting IPXWAN Services	2-3
Starting RIP	2-5
Starting SAP	2-5

For conceptual information about IPX, see Chapter 1, “IPX Concepts”. For information about customizing the way IPX runs on the router, see Chapters 3 through 5.

This chapter assumes that you have read *Using the the Bay Command Console (BCC).*

Starting IPX

To start IPX on the router, you must:

1. Configure a physical interface on an available slot/connector.
2. Configure an IPX interface on the physical interface.

Step 1: Configuring a Physical Interface

To configure a physical interface on a slot and connector, navigate to the top-level box prompt and enter:

interface_type **slot** *slot_number* **connector** *connector_number*

interface_type is the name of a link module on the router.

slot_number is the number of the slot on which the link module is located.

connector_number is the number of a connector on the link module.

For example, the following command configures an Ethernet interface on slot 2, connector 2:

```
box# ethernet slot 2 connector 2
ethernet/2/2#
```

Step 2: Configuring an IPX Interface

To configure an IPX interface on a physical interface, navigate to the prompt for the physical interface and enter:

ipx address *address*

address is a valid IPX address expressed in hexadecimal notation.

For example, the following command configures IPX interface 0x2222 on an Ethernet physical interface on slot 2, connector 2:

```
ethernet/2/2# ipx address 0x2222
ipx/00002222#
```

An IPX interface is now configured on the Ethernet interface with default values for all interface parameters. When you configure an IPX interface, the BCC also configures IPX globally on the router with default values for all IPX global parameters.

You customize IPX by modifying IPX global and interface parameters as described in Chapter 6, “Customizing IPX.”

Starting IPXWAN Services

To start IPXWAN on the router, you must:

1. Configure a WAN physical interface on an available slot/connector.
2. Configure a WAN protocol on the physical interface.
3. Configure an IPXWAN interface over the WAN protocol.

Step 1: Configuring a Physical Interface

To configure a physical interface on a slot and connector, navigate to the top-level box prompt and enter:

interface_type **slot** *slot_number* **connector** *connector_number*

interface_type is the name of a link module on the router.

slot_number is the number of the slot on which the link module is located.

connector_number is the number of a connector on the link module.

For example, the following command configures a serial interface on slot 3, connector 2:

```
box# serial slot 3 connector 2
serial/3/2#
```

Step 2: Configuring a WAN Protocol

Before you can configure IPXWAN services, you must configure a WAN protocol. To configure a WAN protocol, navigate to the prompt for the physical interface and then configure the WAN protocol on the physical interface.

For example, the following commands configure PPP on a serial interface on slot 3, connector 2:

```
box# serial slot 3 connector 2
serial/3/2# ppp
ppp/3/2#
```

Step 3: Configuring an IPXWAN Interface

To configure IPXWAN, navigate to the prompt for the WAN protocol and enter:

ipxwan address *ipxwan_address* **router-name** *name* **primary-network** *address* **negotiated-protocol** *protocol*

ipxwan_address is the address, in hexadecimal notation, of the IPXWAN interface.

name is the symbolic name of the router.

address is the address, in hexadecimal notation, of the primary network.

protocol is one of the following:

wan-rip
unnumbered-rip
wan-unnumbered-rips

For example, the following command configures an IPXWAN interface on a serial interface running PPP on slot 3, connector 2:

```
box# serial slot 3 connector 2
serial/3/2# ppp
ppp/3/2# ipxwan
ppp/3/2# ipxwan 0x543 router-name myrouter primary-net 0x555
ppp/3/2# negotiated-protocol wan-rip
```

An IPXWAN interface is now configured on the serial interface with default values for all interface parameters. When you configure an IPXWAN interface, the BCC also configures IPX globally on the router with default values for all IPX global parameters.

You customize IPXWAN by modifying IPX global and IPX interface parameters as described in Chapter 6, “Customizing IPX.”

Starting RIP

You start RIP on the router by adding RIP to an existing IPX interface.

To start RIP, navigate to an IPX interface-specific prompt and enter:

rip

For example, the following command adds RIP to IPX interface 0x2222:

```
ipx/00002222# rip
rip/00002222#
```

RIP is now running on the router and on the interface with default values for all parameters. You customize RIP by modifying RIP parameters as described in Chapter 6, “Customizing IPX.”

Starting SAP

You start SAP on the router by adding SAP to an existing IPX interface.

To start SAP, navigate to an IPX interface-specific prompt and enter:

sap

For example, the following command adds SAP to IPX interface 0x2222:

```
ipx/00002222# sap
sap/00002222#
```

SAP is now running on the router and on the interface with default values for all parameters. You customize SAP by modifying SAP parameters as described in Chapter 6, “Customizing IPX.”

Chapter 3
Starting IPX Services Using Site Manager

This chapter shows you how to use Site Manager to perform a basic configuration -- that is, a configuration using all available defaults -- for the IPX services described in this guide.

Topic	Page
Starting IPX	3-2
Starting IPXWAN Services	3-3
Starting RIP and SAP Services	3-4

For conceptual information about IPX, see Chapter 1, “IPX Concepts.” For information about customizing the way IPX runs on the router, see Chapters 3 through 5.

This chapter assumes that you have read *Configuring and Managing Routers with Site Manager.*

Starting IPX

Before you can start IPX, you must configure a circuit that IPX can use as an interface to an attached network. For information and instructions, see *Configuring WAN Line Services* and *Configuring Ethernet, FDDI, and Token Ring Services*.

When you have successfully configured the circuit, the Select Protocols window opens. Proceed as follows:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, choose **IPX** or select **RIP/SAP** (which automatically selects IPX) and click on **OK.**	The IPX Configuration window opens.
2. Set the **Configured Network Number (hex)** parameter**.** Click on **Help** or see the parameter description on page B-3.	
3. Click on **OK**.	You return to the Configuration Manager window.

You provide the same information when configuring IPX to run over a LAN or WAN. To customize IPX to run over a LAN, see Chapter 4, “Customizing IPX for LAN Media.” To customize IPX to run over a WAN, see Chapter 5, “Customizing IPX for WAN Media.”

Starting IPXWAN Services

Before you can start IPXWAN, you must configure a circuit that IPXWAN can use as an interface to an attached network. For information and instructions, see *Configuring WAN Line Services*.

When you have successfully configured the circuit, the Select Protocols window opens. Proceed as follows:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, choose **IPX** and click on **OK.**	The IPX Configuration window opens.
2. Set the following parameters: • **IPXWAN** • **Common Network Number** • **Negotiated Protocol(s)** Click on **Help** or see the parameter descriptions beginning on page B-5.	
3. Click on **OK**.	The IPXWAN Configuration window opens.
4. Set the following parameters: • **Router Name** • **Primary Net Number (hex)** Click on **Help** or see the parameter descriptions beginning on page B-7.	
5. Click on **OK**.	You return to the Configuration Manager window.

For information about IPXWAN and how to customize IPX to run over a WAN, see Chapter 5, “Customizing IPX for WAN Media.”

Starting RIP and SAP Services

If you did not start RIP and SAP when you started IPX, you can add them to an existing interface. You start RIP and SAP by adding them to an existing interface.

To add RIP and SAP to an IPX interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the connector on which you want to add RIP and SAP services.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens.
5. Select **RIP/SAP** and click on OK.	You return to the Circuit Definition window.
6. Choose **File**.	The File menu opens.
7. Choose **Exit**.	You return to the Configuration Manager window.

If you do not configure RIP for a WAN interface, you must configure adjacent hosts for all transmission paths to nodes adjacent to frame relay, ATM, or SDMS circuits when you configure an IPX interface. You must then configure static routes that use the adjacent hosts to reach next-hop hosts. For more information about static routes and adjacent hosts, see “Using Static Routes” on page 6-110 and “Configuring an Adjacent Host for an Interface” on page 6-92.

Deleting RIP and SAP from an IPX Interface

To delete RIP and SAP from an IPX interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the connector from which you want to delete RIP and SAP services.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens. The RIP/SAP button is highlighted to show that RIP and SAP are enabled on the circuit.
5. Select and click on OK.	Site Manager deletes RIP and SAP services from the connector. You return to the Circuit Definition window.
6. Choose **File**.	The File menu opens.
7. Choose **Exit**.	You return to the Configuration Manager window.

Customizing RIP and SAP

The instructions in this chapter show you how to start RIP and SAP using all default values and settings. For information about modifying RIP defaults, see “Customizing RIP Parameters” on page 6-38. For information about modifying RIP defaults, see “Customizing SAP Parameters” on page 6-56.

Chapter 4
Customizing IPX for LAN Media

You can use IPX services over either a LAN or a WAN. This chapter relates specifically to using IPX over a LAN. For information specific to using IPX over a WAN, see Chapter 5, “Customizing IPX for WAN Media.” For information about customizing IPX features for both LANs and a WANs, see Chapter 6, “Customizing IPX.”

Topic	Page
Specifying Multiple Interfaces per Circuit	4-1
IPX Host ID Numbers	4-5
Configuring a Multiple-Host Router	4-7
Configuring a Single-Host Router	4-9
Customizing IPX	4-11

Specifying Multiple Interfaces per Circuit

You can configure one or more IPX interfaces per physical circuit. The number of IPX logical interfaces you can configure on a circuit equals the number of unique frame formats available for that circuit type. (See Table 1-1 on page 1-4 for details on circuit types and frame formats.)

For example, the Bay Networks router supports four unique frame formats that are suitable for communication over an Ethernet LAN segment. Therefore, you can configure four *different* encapsulation types (Ethernet, Novell, LSAP, and SNAP) for four independent IPX interfaces on a single Ethernet circuit. Each interface and encapsulation type configured on a circuit support a different logical network. To differentiate between IPX interfaces configured on the same physical circuit,

the Bay Networks router uses the unique network address and frame format that you assign to each interface.

By supporting multiple IPX interfaces on a single physical circuit, a Bay Networks router can service clients on independent logical LANs that coexist on the same physical LAN segment.

In Figure 4-1, each client workstation on the right side of the router has a different logical network address and uses a different encapsulation method. If all clients need to access server 1, then only router interface 2 needs to support all the different encapsulation types and multiple logical network addresses for the workstations. Router interface 1 needs to support only the SNAP encapsulation type that server 1 supports.

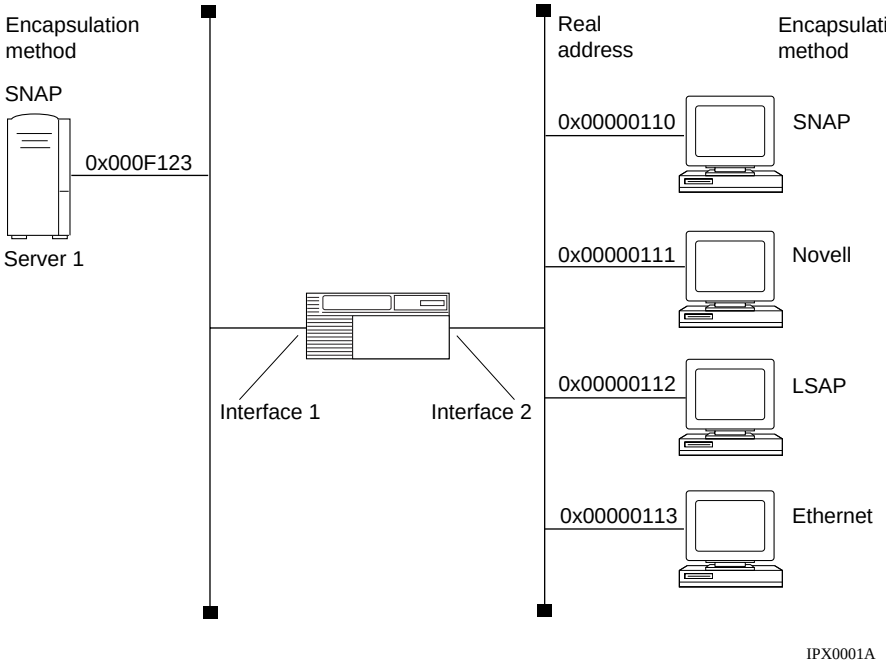

Figure 4-1. Multiple IPX Interfaces per Physical Circuit

Note: If you are upgrading client and server stations on your network to Novell NetWare Version 4.*x*, you can use the multiple-interface-per-circuit capability to gradually migrate stations on the same network segment to NetWare Version 4.*x* (that is, from one logical network to another, independent logical network). For example, you can upgrade and migrate NetWare clients from a logical network that supports only Novell (802.3) encapsulated frames to a logical network that supports a more versatile LSAP (802.2) frame type.

To specify the encapsulation method, see "Choosing a Frame Encapsulation Type" on page 4-1.

Using the BCC

To configure multiple interfaces on a single circuit, you must specify a unique encapsulation type for each interface. To configure multiple interfaces, navigate to the circuit prompt (for example, **box; ethernet 2/1**) and enter:

ipx address *address*; **encapsulation** *type*

address is the address, in hexadecimal notation, of the IPX interface.

type is one of the following:

lsap
ethernet
novell
snap
ppp

For example, to configure two interfaces on a single circuit, enter:

```
ethernet 2/1# ipx 0x0001; encapsulation lsap
ethernet 2/1# ipx 0x0002; encapsulation ethernet
```

Using Site Manager

Site Manager automatically assigns a circuit identifier to each circuit that you create on an IPX router. You can assign a specific circuit identifier, if necessary.

To assign a circuit identifier, complete these tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces.**	The IPX Interface window opens.
4. Set the **Circuit Index** parameter. Click on **Help** or see the parameter description on page B-5.	
5. Click on **OK**.	You return to the Configuration Manager window.

IPX Host ID Numbers

On Bay Networks routers, the IPX host ID number maps to a physical data link layer address on a specific circuit or physical interface. An IPX logical interface can listen at this address and capture frames transmitted by nodes compatible with IPX on the local data link.

Figure 4-2 illustrates this concept using a Bay Networks router that has two IPX logical interfaces, each one configured on a different physical circuit.

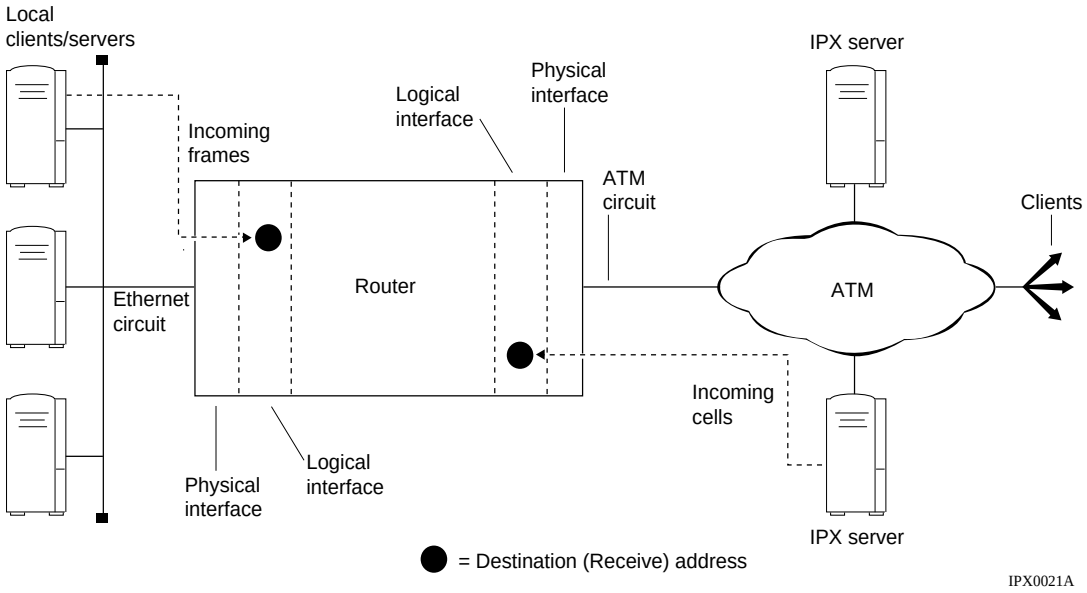

Figure 4-2. Frames Received at a Logical Interface

IPX-compatible nodes on the same logical network and locally attached physical segment must use the host ID number of the IPX logical interface as a data link layer destination address, through which any transmitted frames can ultimately reach their target client or server applications.

Because an IPX logical interface can receive and send data, the host ID also identifies a source data link layer address from which the interface can send frames to nodes compatible with IPX anywhere else in the same IPX internetwork.

Figure 4-3 illustrates this concept using a Bay Networks router configured with two IPX logical interfaces, each one on a different physical circuit type.

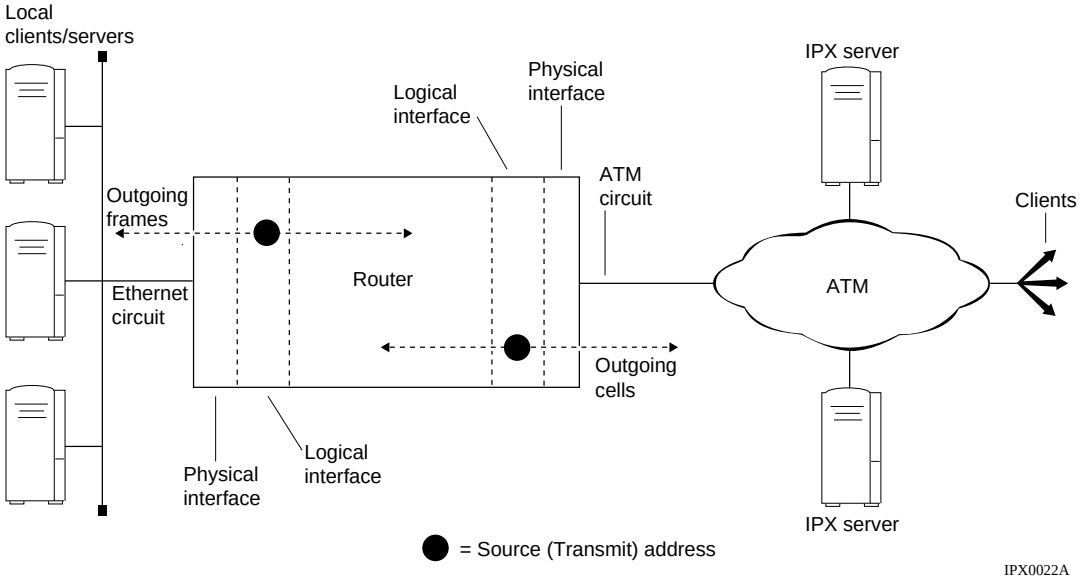

Figure 4-3. Frames Sent from a Logical Interface

Setting an IPX Host ID Number on a Token Ring Circuit

In a configuration with IPX logical interfaces on a token ring circuit, the data link layer address is a MAC-layer address.

On Bay Networks routers, you set the MAC-layer address for the circuit and the host ID number for the IPX interface independently. However, the host ID number for every IPX logical interface on a given token ring circuit must be identical to the MAC address set for that circuit. Otherwise, the logical interface sends frames that contain an incorrect source MAC address, or the interface listens for frames at the wrong MAC address.

Configuring a Multiple-Host Router

A multiple-host router is a common configuration that supports one IPX interface per circuit; each interface has a unique IPX host number. For this configuration,

For this configuration, you must enable multiple host addressing (this is the default setting).

When you enable multiple-host addressing, an IPX interface can use either of the following as a host address:

- The MAC address located in the PROM on the circuit associated with that interface.
- A MAC address that you enter for the multiple host address for that interface. Interfaces on a token ring circuit adopt a host ID number based only on the MAC address of the associated circuit.

If you enter a host number, the circuit adopts that value as the MAC address at which this interface can receive frames. (The MAC address configured at the circuit/line level remains effective for all other interfaces configured on the same circuit.)

Using the BCC

To enable multiple host addressing, navigate to the global IPX prompt (for example; **box; ipx**) and enter:

multiple-host enabled

If you want to o assign a host number to an IPX interface, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

host-address *number*

number is a valid host address in hexadecimal format.

For example, the following command assigns the host address 0x0987 to the IPX interface:

```
ipx/00023456# host-address 0x0987
```

Using Site Manager

To enable multiple-host addressing, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The Edit IPX Global Parameters window opens
4. Set the **Multiple Host Address Enable** parameter to **Enable**. Click on **Help** or see the parameter description on page B-10.	
5. Click on **OK**.	You return to the Configuration Manager window.

If you want to assign a host number to an interface on a multiple-host router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **Host Number (hex)** parameter. Click on **Help** or see the parameter description on page B-25.	
5. Click on **OK**.	You return to the Configuration Manager window.

Configuring a Single-Host Router

To configure a single-host router, you must disable multiple-host addressing.

Disabling multiple host addressing causes all IPX interfaces to adopt a single host ID number for the entire host, based either on the serial number of the router backplane or on a number that you enter in the Host Number parameter field.

Using the BCC

To disable multiple host addressing, navigate to the global IPX prompt (for example; **box; ipx**) and enter:

multiple-host disabled

If you want to assign a host number for all interfaces on a single-host router, navigate to the global IPX prompt (for example, box;ipx) and enter:

host-address *address*

address is the host address in hexadecimal format.

For example, to set the host ID to 0x09873452, enter:

`ipx#` **host-address 0x000009873452**

Using Site Manager

To disable multiple-host addressing, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The Edit IPX Global Parameters window opens
4. Set the **Multiple Host Address Enable** parameter to **Disable**. Click on **Help** or see the parameter description on page B-10.	
5. Click on **OK**.	You return to the Configuration Manager window.

If you want to assign a host number for all interfaces on a single-host router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The IPX Global Parameters window opens.
4. Set the **Router Host Number (hex)** parameter. Click on **Help** or see the parameter description on page B-11.	
5. Click on **OK**.	You return to the Configuration Manager window.

Token Ring MAC Address Selection

For token ring circuits, you can select the means by which the router determines the MAC address for a circuit to one of the following:

- PROM

  The circuit retrieves the MAC address that is stored in a PROM on the supporting link module.

- BOXWIDE

  The circuit generates a MAC address based on the serial number of the backplane of the router.

Caution: The IPX global host address and the token ring MAC address must agree when multiple-host addressing is disabled.

- CNFG

  You can configure a MAC address.

Caution: Changing the way the router determines the MAC address to accommodate IPX configuration requirements can affect other protocol interfaces (for example, LNM Servers or IP) configured on the same circuits with IPX. If necessary, make adjustments to any such non-IPX interfaces configured on the router.

If you choose CNFG, you must enter a valid MAC address override setting. You must repeat this procedure for any token ring circuit for which you choose CNFG (user-configured) as the source for the MAC address assigned to the individual physical circuit. For instructions on how to set the MAC address and the MAC address override, see *Configuring Ethernet, FDDI, and Token Ring Services.*

Customizing IPX

After selecting a circuit and providing the basic IPX settings, your circuit is operational. The default values supplied for the remaining settings apply to most environments. However, if you want to customize your IPX configuration, see Chapter 6, “Customizing IPX.”

Chapter 5
Customizing IPX for WAN Media

You can use IPX services over either a LAN or a WAN. This chapter relates specifically to customizing IPX for use over a WAN. For information about using IPX over a LAN, see Chapter 4, “Customizing IPX for LAN Media.” For information about customizing IPX features for both LANs and WANs, see Chapter 6, “Customizing IPX.”

When you configure IPX over WAN media, you can either configure IPX over a WAN protocol or you can configure IPXWAN services. This chapter includes the following information:

Topic	Page
IPX over WAN Media	5-2
Identifying a Circuit	5-4
Entering an IPX Host ID Number for IPX	5-4
Disabling and Reenabling IPXWAN for an Interface	5-7
Sample IPXCP and IPXWAN Configurations	5-12
IPXCP Link Negotiation	5-13
IPXWAN Link Negotiation	5-13
IPXWAN and IPXCP Link Configurations	5-14

IPX over WAN Media

You can establish an IPX connection over any of the WAN media types supported by the Bay Networks IPX router (see Table 1-2 on page 1-4). The choice of protocols depends on the type of connection and what you want the protocol to do.

The WAN Point-to-Point Protocol (PPP) uses the IPXCP protocol (RFC 1552). IPXCP supports the routing of IPX packets over wide area links that support only PPP. IPXCP is a data link protocol that is part of PPP. To enable IPXCP, you must first configure the interface to support PPP. For instructions on how to do this, see *Configuring PPP Services.*

For the ATM, SMDS, X.25 PDN, X.25 Point-to-Point, and Bay Networks Point-to-Point protocols, only one encapsulation method is allowed for all WAN protocols.

For the frame relay and PPP WAN protocols, you can optionally run IPXWAN (RFC 1634).

Note: Use IPXCP or IPXWAN when you want the routers to negotiate the options required for communication over the WAN link. Alternatively, you can explicitly specify the values for the WAN link without using either IPXCP or IPXWAN, as long as you ensure that the values you configure at each end of the link are compatible.

Using IPXCP and IPXWAN

Incorporating IPXWAN in the Bay Networks router provides the following benefits:

- Adherence to RFCs 1362 and 1634 IPXWAN protocols developed by Novell
- A common link negotiation method for WAN media (frame relay and PPP)
- Interoperability with other routing vendors (for example, Novell)
- A standardized means for tick-based routing over WAN media

If you configure a local and a remote node to support both IPXCP and IPXWAN, IPXCP always runs first. After the router completes IPXCP negotiation, it discards all IPXCP-negotiated options, and IPXWAN runs. See "Identifying a Circuit" on page 5-4 for more information about specifying support for IPXCP and IPXWAN.

Running IPXWAN over PPP

IPX uses PPP when operating over point-to-point synchronous networks. With PPP, establishing a connection means that the IPX Control Protocol (IPXCP) reaches the open state.

PPP lets either side of a connection stop forwarding IPX packets if one end sends an IPXCP terminate request. When a router detects this condition, it immediately reflects the lost connection in its routing information database.

Running IPXWAN over Frame Relay Permanent Virtual Circuits

When you fun IPXWAN over a frame relay PVC, the router encapsulates each IPX packet in a frame relay frame. When you restart an interface, IPXWAN exchanges begin immediately over active, direct-mode frame relay PVCs (those that have remained active before and after restart).

- When a router detects that a direct-mode frame relay PVC has gone from an inactive to an active state, the connection is established; IPXWAN packet exchange over this newly activated connection begins.
- When an active PVC becomes inactive, the router reflects the lost connection in its routing information database.

Note: For IPX, you can use frame relay direct, group, or hybrid mode. For IPXWAN, only direct mode is valid. In frame relay, direct mode is a point-to-point connection. Frame relay group mode (or hybrid mode) involves a point-to-multipoint connection.

Negotiating an IPXWAN Connection

Establishing an IPXWAN connection involves negotiating which router will be the server. The server is the requestor in the ensuing request/response exchanges. A router retains its role -- server or client -- for the remainder of the IPXWAN exchanges. The following options are determined after successful negotiation by the IPXWAN protocol:

- WAN link delay used in tick-based routing across the WAN link
- Network number for the WAN link
- Routing protocol to be implemented over the WAN link

Identifying a Circuit

Site Manager automatically assigns a circuit identifier to each circuit that you create on an IPX router. You can assign a specific circuit identifier, if necessary.

You can assign circuit identifiers only by using Site Manager.

To assign a circuit identifier, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces.**	The IPX Interface window opens.
4. Set the **Circuit Index** parameter. Click on **Help** or see the parameter description on page B-5**.**	
5. Click on **OK**.	You return to the Configuration Manager window.

Entering an IPX Host ID Number for IPX

To establish an IPX connection over an ATM network, you must assign a unique host ID number to the ATM interface that is running IPX. To assign a number, you can either :

- Specify a host address for the interface.
- Specify that the global MAC address be used for the host ID disabling multiple-host addressing.

Using the BCC

To establish an IPX connection over an ATM network if you plan to use multiple-host addressing, navigate to the IPX interface prompt (for example, **box; ipxwan 00023456**) and enter:

host-address *number*

number is a valid host address in hexadecimal format.

For example, the following command assigns the host address 0x0987 to the IPX interface:

```
ipxwan 00055555# host-address 0x0987
```

If you do not plan to use multiple-host addressing and want to use the global MAC address as the host number, navigate to the IPX interface prompt (for example **box; ipx**), and enter:

multiple-host disabled

For example:

```
ipx# multiple-host disabled
```

Using Site Manager

To establish an IPX connection over an ATM network, you can disable multiple-host addressing by:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global.**	The IPX Edit Global Parameters window opens.
4. Set the **Multiple Host Address Enable** parameter to **Disable**. Click on **Help** or see the parameter descriptions on page B-11.	
5. Click on **OK**.	You return to the Configuration Manager window.

To establish an IPX connection over an ATM network when you want to use multiple-host addressing, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **Host Number (hex)** parameter. Click on **Help** or see the parameter description on page B-25.	
5. Click on **OK**.	You return to the Configuration Manager window.

Disabling and Reenabling IPXWAN for an Interface

To run the IPXWAN protocol over a WAN, you must enable IPXWAN on the IPX interface (see Chapter 2 or Chapter 3). Enabling IPXWAN provides a common link negotiation method and a standard means for tick-based routing for WAN media.

When you first configure IPXWAN on an interface, the router automatically enables IPXWAN. You can disable and reenable IPXWAN.

Using the BCC

To disable IPXWAN, navigate to the ipxwan prompt (for example, **box; serial 3/1; ppp; ipxwan 00055555**) and enter:

state disabled

To enable ipxwan, navigate to the ipxwan prompt (for example, **box; serial 3/1; ppp; ipxwan 00055555**) and enter:

state enabled

Using Site Manager

To enable or disable IPXWAN, complete the following tasks:.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **IPXWAN** parameter. Click on **Help** or see the parameter description on page B-5.	
5. Click on **OK**.	You return to the Configuration Manager window.

Assigning a Primary Network Number

Like Novell routers and servers, a Bay Networks router running the IPXWAN protocol implements a global “internal network,” to which you must assign a priimary network number. IPXWAN requires the primary network number to determine whether the local or the remote router on a WAN link serves as the master or slave during the IPXWAN negotiations. The router with the higher primary network number serves as the master.

Using the BCC

You can specify the primary network number only when you configure IPXWAN services. Once you supply the primary network number, you cannot change it. To configure IPXWAN services, see “Starting IPXWAN Services” on page 2-3.

To determine the current primary network number, navigate to the IPXWAN prompt (for example, **box; serial 3/1; ppp; ipxwan 00055555**) and enter:

primary-network ?

Using Site Manager

To specify the primary network number, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Enable IPXWAN**.	The IPXWAN Configuration window opens.
4. Set the **Primary Network Number** parameter. Click on **Help** or see the parameter description on page B-8**.**	
5. Click on **OK**.	You return to the Configuration Manager window.

Entering a Router Name

Every IPX router can have a router name. During IPXWAN negotiations, the local and remote routers provide each other with their respective router names. Once the link is established, the name lets a router know whom it is connected to. Router names are particularly helpful for network management purposes. A symbolic name, such as “printserv,” has more meaning than just a string of digits.

The router name can be up to 47 characters long and can contain the characters A through Z, a through z, 0 through 9, and the special characters underscore (_), hyphen (-), slash (/), and at (@) signs. Some valid names include:

- AAaabbBBxxXXXS/1234
- myrouter@first_floor
- Chicago_office

Using the BCC

You can assign a router name to the remote route only when you configure IPXWAN services. Once you supply the router name, you cannot change it. To configure IPXWAN services, see “Starting IPXWAN Services” on page 2-3.

To determine the current router name, navigate to the IPXWAN prompt (for example, **box; serial 3/1; ppp; ipxwan 00055555**) and enter:

router-name ?

Using Site Manager

To specify the router name, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Enable IPXWAN**.	The IPXWAN Configuration window opens.
4. Set the **Router Name** parameter. Click on **Help** or see the parameter description on page B-7.	
5. Click on **OK**.	You return to the Configuration Manager window.

Indicating the Protocol Negotiated for an Interface

When you specify an IPXWAN interface on a circuit, you must indicate the protocol negotiated for this interface.

Using the BCC

You can determine the negotiated protocol only when you configure IPXWAN services. Once you supply the negotiated protocol, you cannot change it. To configure IPXWAN services, see “Starting IPXWAN Services” on page 2-3.

To determine the current negotiated protocol, navigate to the IPXWAN prompt (for example, **box; serial 3/1; ppp; ipxwan 00055555**) and enter:

negotiated-protocol ?

Using Site Manager

To specify the negotiated protocol, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **Negotiated Protocol** parameter. Click on **Help** or see the parameter description on page B-6.	
5. Click on **OK**.	You return to the Configuration Manager window.

Sample IPXCP and IPXWAN Configurations

Figure 5-1 shows a local router communicating with remote router 1 using IPXCP over PPP, and the same local router communicating with remote router 2 using IPXWAN over frame relay.

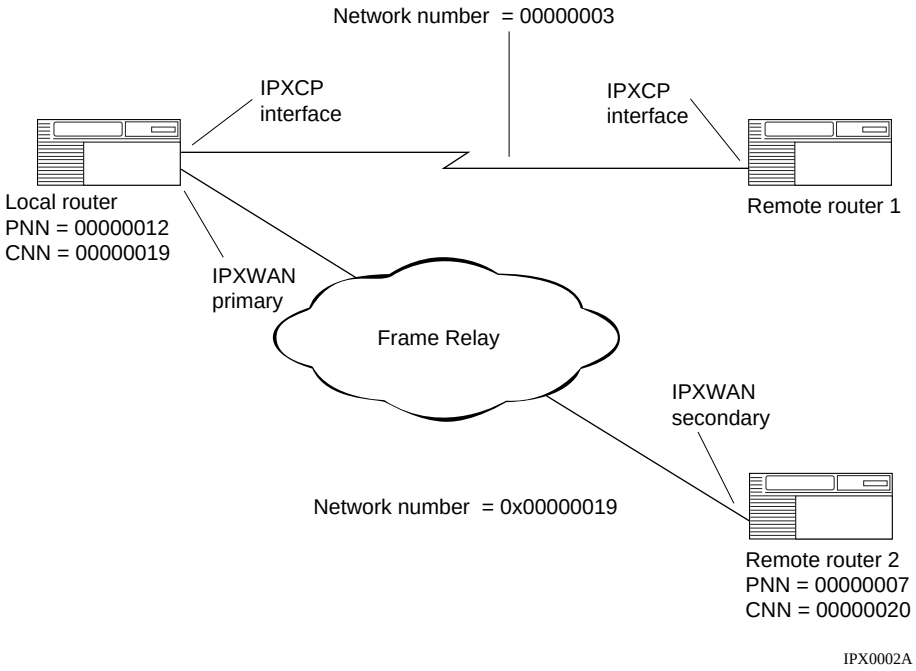

Figure 5-1. IPXCP and IPXWAN Configurations

IPXCP Link Negotiation

In Figure 5-1, the local router and remote router 1, both configured for IPXCP, negotiate a connection at the data link layer. After the options are successfully negotiated, the IPXCP interfaces on both the local router and remote router 1 must agree on a unique network number. When you initially configure an IPXCP interface, you assign an IPX network number to that interface. The routers select the higher of the two IPX network numbers. For instructions on configuring the IPX network number for an IPXCP interface, See *Configuring PPP Services*.

Note: For PPP communication between a Bay Networks IPX Router running Version 7or later and a Bay Networks Version 5 IPX router (or any other vendor's router that does not support IPXCP negotiations), you must manually configure the network number of the IPX interface on both routers.

IPXWAN Link Negotiation

The local router and remote router 2 are both configured for IPXWAN. When you initially configure an IPXWAN interface, you assign a primary network number (PNN) to the router. The router with the highest PNN becomes the server during IPXWAN negotiations on that WAN link.

In Figure 5-1, the local router (PNN=00000012) is the server, and remote router 2 (PNN=00000007) is the client. During the IPXWAN negotiations, both routers negotiate their link options. If successful, the CNN configured for the interface on the server becomes the IPX network number for the WAN link.

After the IPXWAN negotiations are successful on the WAN link, each router can advertise information in its routing/forwarding tables.

IPXWAN and IPXCP Link Configurations

Table 5-1 shows the various WAN protocol configurations likely to exist within local and remote IPX router interfaces. Find the configuration that applies to your situation and read the corresponding description.

Table 5-1. Configuration Table for IPX over WAN Media

	Remote IPX Interface			
Local IPX Interface	**IPXWAN with IPXCP**	**IPXWAN but not IPXCP**	**PPP with IPXCP; no IPXWAN**	**PPP without IPXCP; no IPXWAN**
IPXWAN with IPXCP	Configuration 1	Configuration 2	Configuration 3	Configuration 4*
IPXWAN but not IPXCP	Configuration 2	Configuration 2	Configuration 4	Configuration 4
PPP with IPXCP; no IPXWAN	Configuration 3	Configuration 4	Configuration 3	Configuration 4
PPP without IPXCP; no IPXWAN	Configuration 4*	Configuration 4	Configuration 4	Configuration 4
* Bay Networks Version 7 or later to Bay Networks Series 5.*x* IPX Router Compatibility				

Configuration 1 (IPXWAN with IPXCP on Both Interfaces)

In this configuration, IPXWAN defers to IPXCP for link negotiation:

- IPXWAN negotiation supersedes IPXCP negotiation, regardless of whether IPXCP negotiation succeeds.
- If IPXWAN negotiates successfully, the IPX interface becomes active. If IPXWAN negotiation fails, the IPX interface cannot become active.

Configuration Guidelines -- Configuration 1

- IPXCP -- Use the value 0 for the IPX network number when configuring the local and remote PPP interface.
- IPXWAN -- Specify a unique router name and PNN in the IPX Global Parameters window when configuring the local routers.

You must enable IPXWAN on the interface. To enable IPXWAN, see “To establish an IPX connection over an ATM network when you want to use multiple-host addressing, complete the following tasks:” on page 5-6.

Configuration 2 (IPXWAN on Both Interfaces)

In this configuration, IPXWAN exclusively negotiates an IPX network number for the link. If IPXWAN negotiates successfully, the IPX interface becomes active. If IPXWAN negotiation fails, the IPX interface cannot become active.

Configuration Guidelines -- Configuration 2

- IPXCP -- No configuration requirements.
- IPXWAN -- Specify a unique router name and PNN in the IPX Global Parameters window when configuring the local and remote routers.

You must enable IPXWAN on the interface. To enable IPXWAN, see “To establish an IPX connection over an ATM network when you want to use multiple-host addressing, complete the following tasks:” on page 5-6.

You must also enter a unique common network number for the IPX interface you just configured; the common network number can be 0 when Unnumbered RIP is configured on both interfaces.

Configuration 3 (IPXCP on Both Interfaces)

In this configuration, IPXCP exclusively negotiates an IPX network number for the link:

- If IPXCP successfully negotiates the network number, the IPX interface becomes active on the link.
- If IPXCP fails to negotiate a network number, the IPX interface cannot become active.

Configuration Guidelines -- Configuration 3

- IPXCP -- Use any valid value for the IPX network number when configuring the local or remote PPP interface.
- IPXWAN -- No configuration requirements.

Configuration 4 (Interfaces Do Not Share IPXCP or IPXWAN)

In this configuration, the lower layer has no means of negotiating an IPX network number for the link. For this reason, you must manually configure the network number of the local and remote IPX interfaces to the same value.

Customizing IPX

After selecting a circuit and configuring the associated WAN parameters, your circuit is operational. The default values set for the remaining parameters apply to most environments. However, if you want to configure a circuit in a particular way, refer to Chapter 6, “Customizing IPX.

Chapter 6
Customizing IPX

In most cases, after you add a circuit and supply the basic LAN or WAN settings described in Chapters 3 and 4, you can accept the default values for the remaining parameters and begin sending packets over the network.

To customize IPX, use the information in the following sections:

Topic	Page
Customizing IPX Global Parameters	6-2
Customizing an IPX Interface	6-21
Choosing a Frame Encapsulation Type	6-25
Customizing RIP Parameters	6-38
Customizing SAP Parameters	6-56
Using Static Services	6-71
Customizing NetBIOS Static Routing	6-92
Configuring an Adjacent Host for an Interface	6-92
Dial Services for IPX	6-101
Configuring Dial-Optimized Routing for IPX	6-106
Using Static Routes	6-110
Using RIP Route Filters	6-118
Using SAP Filters	6-119
Configuring Service Name Filters	6-134
Deleting IPX from the Router	6-147

Customizing IPX Global Parameters

Any IPX interface you add to a physical circuit inherits a default IPX configuration from the global IPX process. Use the information in the following sections to customize the default settings that affect all IPX interfaces.

Setting the Maximum Number of Paths

You can set the maximum number of paths allowed for a given network destination and routing method from 1 to 1,023 paths. Multiple paths to a given destination use more memory than single paths, but provide redundancy. Specifying multiple paths allows for load balancing (see "Specifying the Number of Maximum Path Splits" later in this chapter). Bay Networks recommends that you set the maximum number of paths to the highest number of paths that exist from the router to any destination network, regardless of the cost.

Using the BCC

To set the maximum number of paths, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

maximum-path *integer*

integer is the an integer from 1 to 1,023.

For example, the following command sets the maximum path to 4:

```
ipx# maximum-path 4
```

Using Site Manager

To set the maximum number of paths, complete these tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The Edit IPX Global Parameters window opens.
4. Click on **Advanced**.	The Edit IPX Advanced Global Parameters window opens.
5. Set the **Maximum Path (hex)** parameter. Click on **Help** or see the parameter description on page B-15.	
6. Click on **OK**.	You return to the Configuration Manager window.

Filtering Log Messages

You can filter specified types of log messages. For example, the default setting (Trace) filters out trace messages. The types of log messages that you can filter include:

- None
- Debug
- Info
- Trace
- Debug Info
- Debug Trace
- Info Trace
- Debug Info Trace

Do not change the default value of this parameter unless you are an experienced IPX user. Changing the value of this parameter produces significant global effects on memory allocation within the router, and these changes can significantly affect router performance.

If you are an experienced user, enter a filtering mode that yields a level of performance most appropriate for network applications supported by this router.

Using the BCC

To filter specified types of log messages, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

log-filter *option*

option is one of the following:

debug
info
trace
debug-info
debug-trace
info-trace
debug-info-trace

For example, the following command causes IPX to filter Info messages:

```
ipx# log-filter info
```

Using Site Manager

To specify the filtering mode, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The Edit IPX Global Parameters window opens.
4. Click on **Advanced**.	The Edit IPX Advanced Global Parameters window opens.
5. Set the **Log Filter** parameter. Click on **Help** or see the parameter description on page B-15.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Maximum Number of Equal-Cost Paths

You can specify the maximum number of equal-cost paths over which IPX will do load balancing to a particular destination. For example, if the maximum number of path splits is non-zero, and there are five equal-cost routes to a destination, IPX will distribute the packets over the five paths in a round-robin fashion.

Using the BCC

To specify the maximum number of paths allowed for a given network destination and routing method, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

maximum-path *integer*

integer is the number, between 1 and 1023, of paths.

For example, the following command sets the number of paths to age to 999:

```
ipx# maximum-path 999
```

Using Site Manager

To specify whether the router will do load balancing to a particular destination, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The Edit IPX Global Parameters window opens.
4. Click on **Advanced**.	The Edit IPX Advanced Global Parameters window opens.
5. Set the **Maximum Path** parameter. Click on **Help** or see the parameter description on page B-15.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Maximum Number of Destinations

You can specify the maximum number of destinations (networks) for the router to learn. IPX uses this value to preallocate table sizes for forwarding and network tables. If you use the default value, 0, IPX dynamically allocates the amount of memory it needs for the tables.

Do not change the default unless you are an experienced IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value can significantly affect router performance by affecting the memory usage by IPX and the learning time of the router. If you are an experienced user, enter a value from 0 to 5000 destinations that yields a level of performance most appropriate for network applications supported by this router.

Using the BCC

To set the maximum number of destinations, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

destination-count *integer*

integer is the number of destinations.

For example, the following command sets the maximum number of destinations to 15:

```
ipx# destination-count 15
```

Using Site Manage

To specify the maximum number of destinations for the router to learn, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The Edit IPX Global Parameters window opens.
4. Click on **Advanced**.	The Edit IPX Advanced Global Parameters window opens.
5. Set the **Destination Count** parameter. Click on **Help** or see the parameter description on page B-17.	
6. Click on **OK**.	You return to the Configuration Manager window.

Entering the Maximum Number of Services

You can specify the maximum number of services for the router to learn. IPX uses this value to preallocate table sizes for service tables. If you use the default value, 0, IPX automatically allocates the amount of memory it needs for the tables.

Do not change the default unless you are an experienced IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value can significantly affect router performance by affecting the memory usage by IPX and the learning time of the router. If you are an experienced user, enter a value from 1 to 5000 services that yields a level of performance most appropriate for network applications supported by this router.

Using the BCC

To set the maximum number of services for the router to learn, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

service-count *integer*

integer is the number of services.

For example, the following command sets the maximum number of services to 6:

```
ipx# service-count 6
```

Using Site Manager

To specify the maximum number of services for the router to learn, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The Edit IPX Global Parameters window opens.
4. Click on **Advanced**.	The Edit IPX Advanced Global Parameters window opens.
5. Set the **Service Count** parameter. Click on **Help** or see the parameter description on page B-17.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Aging Time for RIP and SAP Information

You can specify the number of seconds for aging RIP and SAP information. IPX checks whether any routes have timed out every *n* seconds, where *n* is the interval that this parameter specifies. By default, IPX checks for timed-out routes every 10 seconds. You can change this setting to a value from 1 to the maximum positive integer (seconds).

Note: Do not change the default value of this parameter unless you are an experienced IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an experienced user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

Using the BCC

To set the interval for aging RIP and SAP information, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

aging-frequency *integer*

integer is the number of seconds from 1 to the maximum positive integer.

For example, the following command sets the interval for aging RIP and SAP information to 20:

```
ipx# aging-frequency 20
```

Using Site Manager

To specify the interval for aging RIP and SAP information, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The Edit IPX Global Parameters window opens.
4. Click on **Advanced**.	The Edit IPX Advanced Global Parameters window opens.
5. Set the **Aging Frequency** parameter. Click on **Help** or see the parameter description on page B-18.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Aging Pending Frequency

You can specify the number of routes and services to age (process) before pending. A higher number lets the aging process proceed more quickly.

Do not change the default value of 100 unless you are an experienced IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value can significantly affect router performance. If you are an experienced user, enter a value (between 1 and the maximum number of routers and services) that yields a level of performance most appropriate for network applications supported by this router.

Using the BCC

To set the number of routes and services to process before pending, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

pend-frequency *integer*

integer is the number of routes and services from 1 to the maximum number of routes and services.

For example, the following command sets the number of routes and services to age to 100:

```
ipx# pend-frequency 20
```

Using Site Manager

To specify the number of routes and services to process before pending, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The IPX Global Parameters window opens.
4. Click on **Advanced**.	The IPX Advanced Global Parameters window opens.
5. Set the **Aging Pending Frequency** parameter. Click on **Help** or see the parameter description on page B-19.	
6. Click on **OK**.	You return to the Configuration Manager window.

Enabling IPX Default Routing

When you configure IPX on an interface, by default, the router enables the use of the default route 0xFFFFFFFE for IPX routing.

When IPX enables default routing, the router to uses the default route (if one exists in its routing table) when it receives an IPX packet that does not contain a known IPX destination address within the IPX protocol header.

Disabling default routing forces the router to drop a packet whose destination address is unknown, even if a default route exists.

By default, the router uses default routing.

Using the BCC

To disable the use of the default route, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

default-route disabled

To reenable the use of the default route, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

default-route enabled

Using Site Manager

To globally enable or disable the use of the default route for IPX routing, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The IPX Global Parameters window opens.
4. Click on **Advanced**.	The IPX Advanced Global Parameters window opens.
5. Set the **Default Route** parameter. Click on **Help** or see the parameter description on page B-19.	
6. Click on **OK**.	You return to the Configuration Manager window.

Selecting the GNS Response Mode

You can specify which server the router chooses when responding to a get_nearest_server (GNS) request. By default, when a server responds to a get_nearest_server request, the router sorts through all server names alphabetically. You can either accept the default method or specify that the router select the last server learned.

Using the BCC

To specify which server the router chooses when responding to a get_nearest_server request, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

gns-response *option*

option is one of the following:

alphabetical
last-learned

For example, the following command specifies that the router responds to a get_nearest_server request by selecting the last server learned:

```
ipx# gns-response lastlearned
```

Using Site Manager

To specify which server the router chooses when responding to a get_nearest_server request, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The Edit IPX Global Parameters window opens.
4. Click on **Advanced**.	The Edit IPX Advanced Global Parameters window opens.
5. Set the **GNS Response Mode** parameter. Click on **Help** or see the parameter description on page B-21.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Table Fill Notify Value

The table fill notify value causes the IPX router to notify you when the IPX network table is filled. To specify the table fill notify value that is, the number of network table entries, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

table-fill-notify *integer*

integer is any valid integer.

For example, to set the table fill notify value to 500, enter:

```
ipx# table-fill-notify 500
```

Specifying the Size of the Network Table

To specify the size of the network table, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

network-table-size *integer*

integer is any valid integer.

For example, to set the size of the network table to 300, enter:

```
ipx# network-table-size 300
```

Specifying the MIB Reply Slot

To specify the slot where IPX sends MIB replies, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

mib-reply-slot *slot_no*

slot_no is any valid slot number.

For example, to set the MIB reply slot to slot 4, enter:

```
ipx# mib-reply-slot 4
```

Specifying the Routing Method

You can specify a method for making IPX "best-route" decisions for all slots, based on time delays (ticks) incurred or hops encountered for packet delivery.

The router can assess the time delay in one of the following ways:

- *Number of timer ticks*: the amount of time, expressed in ticks, that a packet requires to reach another network segment. Each timer tick equals approximately 1/18th of a second. The maximum configurable number of ticks is 65,534. This value multiplied by 1/18th of a second equals 3600 seconds, or 60 minutes.
- *Number of hops*: the number of router hops a packet can traverse to reach a network segment. The maximum number of hops is 15.

By default, the router assesses the time delay in ticks. If you accept the default and the router knows about two paths to a network, and both paths have equal tick values, the router chooses the path with the smallest number of hops.

If you select hop, and the best route results in the same number of hops, the router makes its decision based only on the number of hops between network segments.

Bay Networks recommends using the default (tick-based) method. Note that every node on the network must use the same routing method.

Using the BCC

To specify the routing method, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

routing-method *method*

method is one of the following:

tick
hop

For example, to specify that IPX use hop-based routing, enter:

```
ipx# routing-method hop
```

Using Site Manager

To specify the routing method, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The Edit IPX Global Parameters window opens.
4. Click on **Advanced.**	The Edit IPX Global Advanced Parameters window opens.
5. Set the **Routing Method** parameter. Click on **Help** or see the parameter description on page B-14.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Maximum Number of Hops

You can specify the maximum number of hops an IPX packet cany take to reach its destination. By default, 16 is the maximum number of hops for an IPX packet to reach a destination. You can set this value from 1 to 255. Every node in the network should use the same maximum number of hops.

Using the BCC

To specify the maximum number of hops, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

hops *hop_count*

hop_count is the number of hops from 1 to 255.

For example, to set the maximum number of hops to 20, enter:

`ipx#` **hops 20**

Using Site Manager

To specify the maximum number of hops for an IPX packet to reach its destination, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The Edit IPX Global Parameters window opens.
4. Click on **Advanced**.	The Edit IPX Advanced Global Parameters window opens.
5. Set the **Maximum Hops** parameter. Click on **Help** or see the parameter description on page B-16.	
6. Click on **OK**.	You return to the Configuration Manager window.

Indicating the Number of Next-Hop Hosts

You can specify the maximum number of next-hop hosts for the router to learn. IPX uses this value to allocate table sizes for host tables. By default, the router learns one next-hop host. You can set this value from 1 to 5000 next-hop hosts.

Do not change the default value of this parameter unless you are an experienced IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value of this parameter can significantly affect the memory used by IPX, but it can also speed learning time for the router. If you are an experienced user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

Using the BCC

To specify the number of next-hop hosts for the router to learn, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

host-count *hosts*

hosts is the number of next-hop hosts from 1 to 5000.

For example, to set the number of next-hop hosts to 20, enter:

`ipx#` **host-count 20**

Using Site Manager

To specify the number of next-hop hosts for the router to learn, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The Edit IPX Global Parameters window opens.
4. Click on **Advanced**.	The Edit IPX Advanced Global Parameters window opens.
5. Set the **Host Count** parameter. Click on **Help** or see the parameter description on page B-18.	
6. Click on **OK**.	You return to the Configuration Manager window.

Customizing an IPX Interface

Any IPX interface you add to a physical circuit inherits a set of default IPX values from the global IPX process. These interface values determine how IPX behaves on individual router interfaces. You can customize the parameters that belong to a specific interface by modifying the values of the IPX interface settings.

Disabling and Reenabling IPX Routing on an Interface

After you add an interface to a circuit, you can disable or reenable IPX routing on this interface. By default, IPX is enabled on an interface.

Reenabling IPX on an interface reinitializes an existing disabled IPX interface. The actual operating state of an interface, once enabled, depends on:

- The current state of the associated circuit
- The current state of the IPX global/slotwide protocol process

Disabling an IPX interfaces forces an IPX interface into the down (inoperative) state.

Using the BCC

To disable IPX routing on an interface, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

state disabled

To reenable IPX routing on an interface, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

state enabled

Using Site Manager

To disable or reenable IPX routing on an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **Enable** parameter. Click on **Help** or see the parameter description on page B-23.	
5. Click on **Apply** and **Done.**.	You return to the Configuration Manager window.

Entering a Symbolic Name for an Interface

You can specify a symbolic name for an interface on a router, for example, first_floor_printer.

See the documentation that came with your NetWare operating system for guidelines on specifying a host, interface, router, or server name. It is a good idea to make the name meaningful to users as well as to routers.

Using the BCC

To specify a symbolic name for an IPX interface on a router, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

circuit-name *name*

name is any meaningful name for an IPX interface.

For example, the following command specifies the name first_floor_printer for an IPX interface:

```
ipx/00023456# circuit-name first_floor_printer
```

Using Site Manager

To specify a symbolic name for an IPX interface on a router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **Name** parameter. Click on **Help** or see the parameter description on page B-23.	
5. Click on **Apply** and **Done**.	You return to the Configuration Manager window.

Assigning a Host Number to an Interface

You can assign a host number to an IPX interface after you enable multiple-host addressing.

If you configured the router as a multiple-host router and want to accept the PROM-based default setting for the MAC address, this IPX interface adopts a host number based on the MAC address of the underlying circuit. In this case, a PROM on the circuit supplies the number for the MAC address of the circuit and the host number of the interface.

You can enter a host number for this interface when:

- Multiple-host addressing is enabled.
- You do not want to accept the default PROM-based setting for the MAC address.
- The circuit type supports only selective mode of operation (such as with Ethernet circuits).

If you enter a host number, the circuit adopts that value as the MAC address at which this interface can receive frames. (The MAC address configured at the circuit/line level remains for all other interfaces configured on the same circuit.)

Using the BCC

To assign a host number to an IPX interface, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

host-address *number*

number is a valid host address in hexadecimal format.

For example, the following command assigns the host address 0x0987 to the IPX interface:

`ipx/00023456#` **host-address 0x0987**

Using Site Manager

To assign a host number to an IPX interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **Host Number (hex)** parameter. Click on **Help** or see the parameter description on page B-25.	
5. Click on **Apply** and **Done.**	You return to the Configuration Manager window.

Choosing a Frame Encapsulation Type

When you add an IPX interface to the router configuration, the router supplies default frame encapsulation type that is dependent on the physical circuit type. You must specify the same type of frame encapsulation for all hosts on the same IPX logical network within the overall IPX internetwork.

Choose the encapsulation method that matches the one that the clients and servers on the same logical network use and is appropriate for the physical circuit you are configuring:

- Ethernet circuits support Ethernet, LSAP, Novell, and SNAP frames.
- Token ring circuits support LSAP and SNAP frames.
- Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21, T1/E1) support SNAP, PPP, and X.25 Point-to-Point (Ethernet) frames.
- FDDI circuits support LSAP and SNAP frames.
- HSSI circuits support PPP and SNAP frames.
- ISDN circuits support PPP frames.

Using the BCC

To specify the encapsulation method, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

encapsulation *method*

method is one of the following:

lsap
ethernet
novell
snap
ppp

For example, the following command sets the encapsulation type to LSAP:

```
ipx/00023456#encapsulation lsap
```

Using Site Manager

To specify the encapsulation method, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **Configured Encaps** parameter. Click on **Help** or see the parameter description on page B-4.	
5. Click on **Apply** and **Done.**	You return to the Configuration Manager window.

Enabling Source Routing for an Interface on a Token Ring Circuit

Source routing enables routable traffic generated in a source route bridge environment to be routed to workstations on remote LANs over a multiprotocol backbone. The Bay Networks router running IPX lets you configure source routing for token ring networks on each interface so that with each source route end-station support enabled, end stations that support both source route bridging and IPX can use source routing to traverse bridged networks.

In a source routing network, every end station supplies each frame it sends out with route descriptors, so that it can be source routed across the network. Thus, for a router running IPX to route packets across a source routing network, the router must act like an end-station, supplying route descriptors within each packet before sending it onto the network.

All traffic is source route bridged within the local token ring environment. Routable traffic intended for a destination on a LAN interconnected through a multiprotocol backbone is routed over the backbone by the Bay Networks node. With end station support enabled, the Bay Networks router running IPX does the following whenever it receives a packet and determines that the packet’s next hop is across a source routing network:

- Sends out a Single Route Explorer (SRE) frame to discover a path to the next-hop network
- Adds the necessary routing information field (RIF) information to the packet's MAC header
- Sends the packet to the network, where it is source routed toward the next hop

After the peer router receives the packet from the token ring network, it strips off the RIF field and continues to route the packet toward the destination network address.

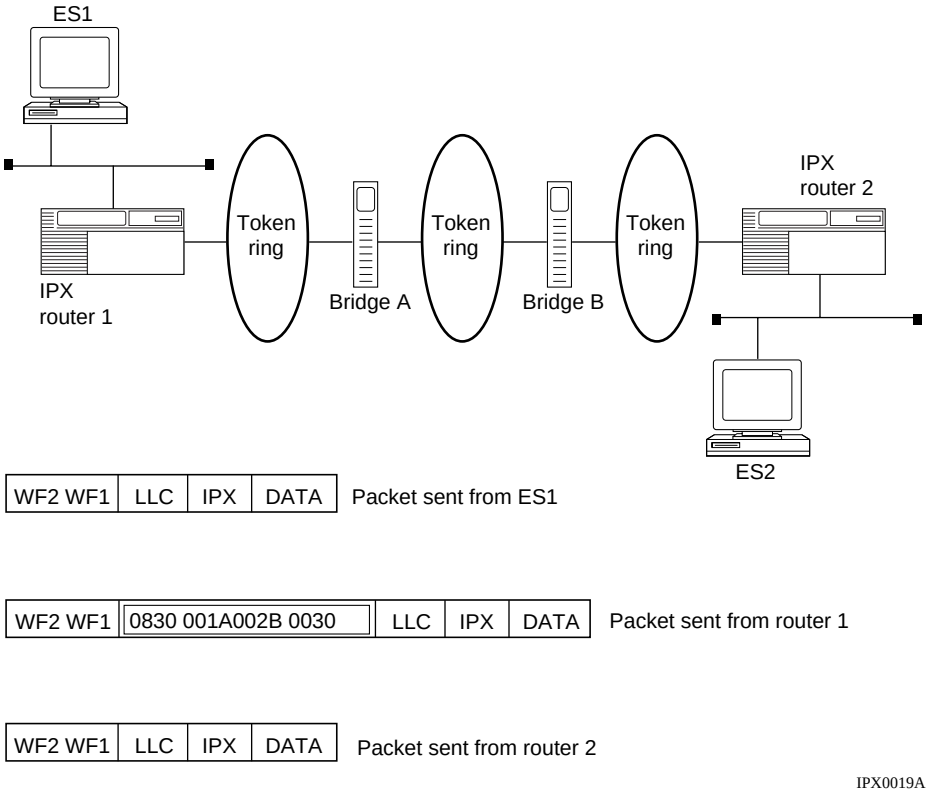

Figure 6-1. IPX Routers Source Routing across a Token Ring Network

The transition to network-layer routing outside the source route bridge environment can improve overall network performance by reducing source route bridge overhead on a WAN and can maximize network availability by rapidly rerouting around a failed link.

When you enable IPX for an interface on a token ring circuit, by default the router disables source routing. Accept the default if you do not want to use source routing over this interface.

You should enable source routing if this interface connects to a bridged token ring network.

Using the BCC

To enable source routing for an IPX interface on a token ring circuit, navigate to the IPX interface prompt (for example, **box; token-ring 2/1; ipx 00023456**) and enter:

end-station enabled

To disable source routing for an IPX interface on a token ring circuit, navigate to the IPX interface prompt (for example, **box; token-ring 2/1; ipx 00023456**) and enter:

end-station disabled

For example, the following command enables source routing on IPX interface 00023456:

```
ipx/00023456# end-station enabled
```

Using Site Manager

To enable or disable source routing for an IPX interface on a token ring circuit, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **TR End Station** parameter. Click on **Help** or see the parameter description on page B-26.	
5. Click on **Apply** and **Done.**	You return to the Configuration Manager window.

Specifying a Broadcast Address

You can specify a WAN broadcast address for an IPX interface. The default value (0xFFFFFFFFFFFF) causes the data link layer to issue a WAN broadcast packet on all active virtual circuits. The value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol.

You accept the default value, or enter a WAN broadcast address to send all broadcast traffic through the IPX interface you are configuring. With the default value, the IPX router sends all broadcast traffic through all logical connections associated with the IPX interface you are configuring. Broadcast traffic includes RIP and SAP broadcasts.

Note that Site Manager does not display the default value 0xFFFFFFFFFFFF.

Using the BCC

To specify a WAN broadcast address for an interface, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

broadcast-address *address*

address is a valid WAN broadcast address in hexadecimal format.

For example, to assign the WAN broadcast address 0x01203406, enter:

`ipx/00023456#` **broadcast-address 0x01203406**

Using Site Manager

To specify a WAN broadcast address for an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **FR Broadcast (hex)** parameter. Click on **Help** or see the parameter description on page B-28.	
5. Click on **Apply** and **Done.**	You return to the Configuration Manager window.

Specifying a Multicast Address

You can specify a WAN multicast address for an IPX interface. The default value (0xFFFFFFFFFFFF) causes the data link layer to issue a multicast packet on all active virtual circuits. The value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol.

You can accept the default value, or enter a WAN multicast address to send all multicast traffic through the IPX interface you are configuring. With the default value, the IPX router sends all multicast traffic through all logical connections associated with the IPX interface you are configuring.

Note that Site Manager does not display the default value 0xFFFFFFFFFFFF.

Using the BCC

To specify a WAN multicast address for an interface, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

multicast-address *address*

address is a valid WAN multicast address in hexadecimal format.

For example, to assign the WAN multicast address 0x01203405, enter:

`ipx/00023456#` **multicast-address 0x01203405**

Using Site Manager

To specify a WAN multicast address for an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **FR Multicast (hex)** parameter. Click on **Help** or see the parameter description on page B-28.	
5. Click on **Apply** and **Done.**	You return to the Configuration Manager window.

Setting the Delay Time

You can specify the length of time, from 0 through 2,147,483,647 microseconds, required to transmit 1 byte of data (excluding protocol headers) to a destination on the other end of this IPX circuit, if the circuit is free of other traffic.

Using the BCC

To specify the maximum amount of time to transmit 1 byte of data, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

delay *microseconds*

microseconds is a value from 0 to 2,147,483,647 microseconds.

For example, to specify that the router should take 10,000 microseconds to transmit 1 byte of date, enter:

`ipx/00023456#` **delay 10000**

Using Site Manager

To specify the amount of time to transmit 1 byte of data, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **Delay** parameter. Click on **Help** or see the parameter description on page B-29.	
5. Click on **Apply** and **Done.**	You return to the Configuration Manager window.

Specifying Throughput

You can specify the maximum amount of data, from 0 to 2,147,483,647 bits per second, that can flow through an IPX circuit if the circuit is free of other traffic.

Using the BCC

To specify the data throughput, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

throughput *bits_per_second*

bits_per_second is an integer from 0 to 2,147,483,647 bits per second.

For example, to specify the data throughput as 1,000,000 bits per second, enter:

`ipx/00023456#` **throughput 1000000**

Using Site Manager

To specify the data throughput, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **Throughput** parameter. Click on **Help** or see the parameter description on page B-30.	
5. Click on **Apply** and **Done.**	You return to the Configuration Manager window.

Setting the Stabilization Timer Delay

You can set the amount of time, from 0 through 2,147,483,647 seconds, that RIP/SAP waits before sending out initial route information when the circuit first becomes active. The more routes that you expect a router to handle or the more dynamic the network is, the higher you should set this value to allow the router enough time to assimilate incoming routes before it sends out an initial update on a circuit.

Using the BCC

To specify the RIP/SAP delay period, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

stabilization-timer *seconds*

seconds is an integer from 0 to 2,147,483,647 seconds.

For example, to set the RIP/SAP delay period to 100,000 seconds, enter:

`ipx/00023456#` **stabilization-timer 100000**

Using Site Manager

To specify the RIP/SAP delay period, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **Stabilization Timer Delay (secs)** parameter. Click on **Help** or see the parameter description on page B-29.	
5. Click on **Apply** and **Done.**	You return to the Configuration Manager window.

Setting a Cost for an Interface

You can set the cost (number of ticks or hops) for an interface. The value you enter depends on whether you selected hops or ticks for the routing method.

By configuring an interface's cost you can select the route you want to use, rather than letting the router select the route. For example, two routes go to the same destination. Route A has a tick cost of 2; route B has a tick cost of 3. Because route A has the lower tick cost, the router selects it as the "best route" to the destination. If you want traffic to go over route B, you can set the tick cost of route A to 4, which then forces traffic to go over route B.

IPX routing decisions can be based on tick values that you define. This allows the implementation of tick-based routing over non-IPX WAN links (for example, HDLC encapsulation), letting you optimize IPX network performance.

In Figure 6-2, for example, traffic generated by end system 1 (ES1) on network A is directed to the IPX server ES2 on network B over interface 2 (route of least tick delay). However, other protocols such as IP, AppleTalk, and OSI will most likely select this route as the least-cost path between network A and network B, as well. Consequently, traffic congestion over this route may preclude it from being the most efficient path between these two network segments.

By specifying the interface cost value, you can assign a lower cost to interface 1 on router 1, so that IPX traffic is routed through interface 1. This lets you maximize IPX internetwork performance between networks A and B, even though it traverses two T1 lines instead of one.

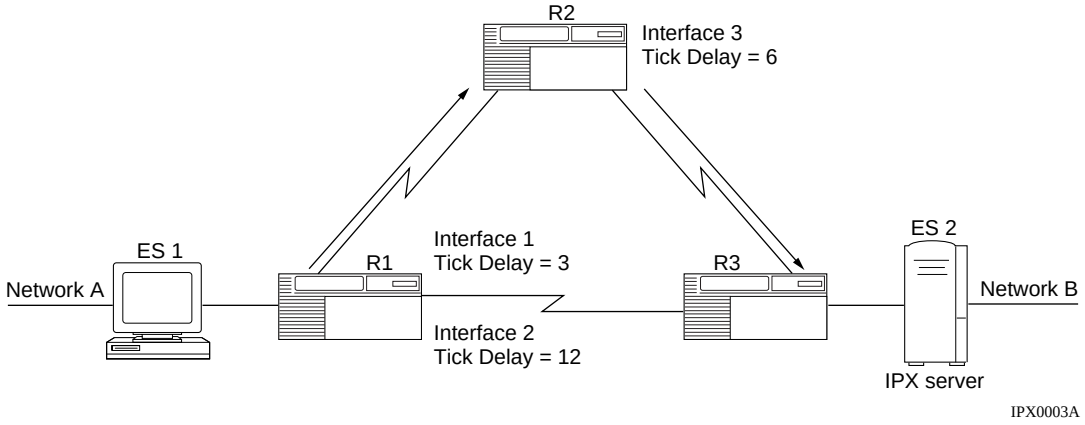

Figure 6-2. IPX Interface Cost

You can set the cost (number of ticks or hops) for an interface. The cost is added to route information learned on this interface through RIP and is included in subsequent RIP packets sent to other interfaces. IPX discards the packet when its hop count exceeds a value that is one less than the maximum number of hops. The cost value must be the same across the network.

For all non-WAN and HSSI interfaces, the default value translates into a tick cost of 1 in the routing table. For all WAN interfaces, the default value translates into a tick cost of 6 in the routing table.

Note: Do not change the default value of this parameter unless you are an experienced IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value of this parameter can significantly affect router performance. If you are an experienced user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

Using the BCC

To specify the routing cost for an interface, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

cost *integer*

integer is 0 to one less than the number of maximum hops for hop-based routing or 0 to the maximum positive integer for tick-based routing.

For example, to set the interface cost to 120, enter:

```
ipx/00023456# cost 120
```

Using Site Manager

To specify the routing cost for an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **Cost** parameter. Click on **Help** or see the parameter description on page B-24.	
5. Click on **Apply** and **Done**.	You return to the Configuration Manager window.

Customizing RIP Parameters

The Routing Information Protocol (RIP) enables workstations and routers to exchange route information and to establish the route to each network with the fewest hops and shortest delay.

Each IPX router maintains a route table. The route table contains the following information about every network in the IPX network topology:

- The network address.
- The number of ticks (units of delay time) to that network. (A tick is equal to 1/18 a second. The number of ticks to a network is the *tick cost* for that route.)
- The number of hops to that network. (A hop is an adjacent router; the number of hops is equal to the number of adjacent routers that a packet must traverse to reach another network segment.)
- The address of the next-hop node to which the local router forwards packets on their way to another destination network.

Routers maintain route tables by exchanging RIP request and response packets. A RIP request packet specifies the destination network. A RIP request packet can be either:

- A general request broadcast by a router to retrieve the fastest route to all known networks on an internetwork. The value 0xFFFFFFFF in the network address field indicates that the packet is a general request.
- A specific request broadcast by a workstation or router to determine the fastest route to a particular network. One or more network addresses (excluding an address of all Fs) in the network address field indicates that the packet is a specific request.

Routers issue RIP response packets. RIP response packets contain the network number and the number of hops and ticks required to get to the network. A RIP response can be one of the following types:

- A response to a request.
- An informational broadcast from a router issued at regular intervals (by default, every 60 seconds).
- An informational broadcast when a change occurs in the routing table. Examples of changes in the routing table are tick or hop changes, timing out of routes, and the addition of routes to the table.
- An informational broadcast when an interface initializes or performs an orderly shutdown procedure.

Each RIP packet can contain up to 50 route updates. To reduce traffic, RIP broadcasts are limited to a router's immediate segments and are not forwarded by receiving routers.

Note: The IPX router learns WAN addresses from RIP and SAP broadcasts received over WANs (frame relay, SMDS, ATM). The router stores IPX address/WAN address pairs for future use as next-hop destinations.

If you enable RIP on an IPX interface, a route filter can still prohibit the interface from updating its internal routing tables (see"Using RIP Route Filters" on page 118).

If you do not configure RIP for a WAN interface, you must configure adjacent hosts for all transmission paths to nodes adjacent to frame relay, ATM, or SMDS circuits when you configure an IPX interface. You must then configure static routes that use the adjacent hosts to reach next-hop routers. Refer to the descriptions of adjacent hosts and static routes in this chapter for more information about these features.

Disabling and Reenabling RIP

When you first configure RIP on an interface, it is automatically enabled.

Using the BCC

To disable RIP, navigate to the IPX RIP prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

state disabled

To reenable RIP, navigate to the IPX RIP prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

state enabled

For example, to disable RIP on IPX interface 0x00023456, enter:

`ipx/00023456#` **state disabled**

Using Site Manager

To disable or reenable RIP, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces.**	The IPX Interfaces window opens.
4. Choose **RIP.**	The IPX RIP Circuit window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page B-36.	
6. Click on **OK**.	You return to the Configuration Manager window.

Enabling RIP Listen and Supply Functions

You can determine whether the IPX router learns routes received in RIP updates from neighboring routers, transmits RIP periodic and triggered updates to routers in adjacent networks, or does both.

By default, the IPX router learns routes from and transmits updates to routers in adjacent networks.

Using the BCC

To specify that IPX not transmit periodic or triggered RIP updates, navigate to the IPX RIP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

supply disabled

To specify that IPX transmits periodic or triggered RIP updates, navigate to the IPX RIP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

supply enabled

For example, to specify that IPX transmits triggered RIP updates, enter:

```
rip/00023456# supply enabled
```

To specify that IPX not learn routes received in RIP updates from neighboring routers, navigate to the IPX RIP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

listen disabled

To specify that IPX learns routes received in RIP updates from neighboring routers, navigate to the IPX RIP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

listen enabled

For example, to specify that the IPX interface learns routes received in RIP updates from neighboring routers, enter:

```
rip/00023456# listen enabled
```

Using Site Manager

To specify whether IPX transmits or receives periodic or triggered RIP updates, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **RIP.**	The IPX RIP Circuit window opens.
5. Set the **Mode** parameter. Click on **Help** or see the parameter description on page B-36.	
6. Click on **OK**.	You return to the Configuration Manager window.

Determining the Pace of RIP Packets

The RIP pace determines the frequency, in packets per second, at which RIP sends out packets on a circuit. By default, RIP sends 18 packets per second on a circuit.

You can specify a RIP pace of 0 to 1000 packets per second. If you enter a value of 0, there is no limit on the pace.

Using the BCC

To specify the RIP pace, navigate to the IPX RIP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

pace *packets_per_second*

packets_per_second is the number of packets, from 0 to 1000, that RIP sends per second.

For example, to set the IPX RIP interface pace to 20 packets per seconds, enter:

`rip/00023456#` **pace 20**

Using Site Manager

To specify the RIP pace, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **RIP.**	The IPX RIP Circuit window opens.
5. Set the **Pace** parameter. Click on **Help** or see the parameter description on page B-37.	
6. Click on **OK**.	You return to the Configuration Manager window.

Configuring RIP Timers

You can extend the standard 60-second periodic IPX RIP advertisement interval. By default, the timeout time is three times the standard 60-second RIP advertisement update interval, or 180 seconds.

Configuring RIP timers can reduce IPX RIP overhead and enhance bandwidth availability. Furthermore, you can eliminate periodic RIP advertisements by setting the configurable RIP timer to 0; thus, only RIP updates triggered by changes in the internetwork topology are propagated.

To ensure proper RIP operation, all configurable RIP timers must be set at equal advertisement intervals on all router interfaces attached to common IPX network segments.

Note: Although you can set configurable RIP timers on any Bay Networks router interface, do not use them on LAN interfaces, because IPX servers do not allow configuration of update timers (with internal routers). As a result, IPX servers will by default purge RIP entries after 180 seconds if they have not received any updates within this 180-second period.

For example, in Figure 6-3, if router R1 is configured to issue periodic RIP advertisements every 240 seconds over interface 1 and router R2 is configured to issue advertisements per the IPX standard (every 60 seconds) over interface 2, then router R2 will purge RIP entries learned through interface 2 every 180 seconds and reinstate them 60 seconds later when it receives a periodic RIP advertisement from router R1. More critically, router R2 will issue triggered RIP updates through interface 3, propagating these unnecessary changes throughout the internetwork behind router R2.

Setting the configurable RIP timers at 240 seconds on both interface 1 on router R1 and interface 2 on router R2 ensures proper RIP operation, because RIP entries are not purged unless an update for a particular entry is not received within a 720-second interval (3 * 240 seconds).

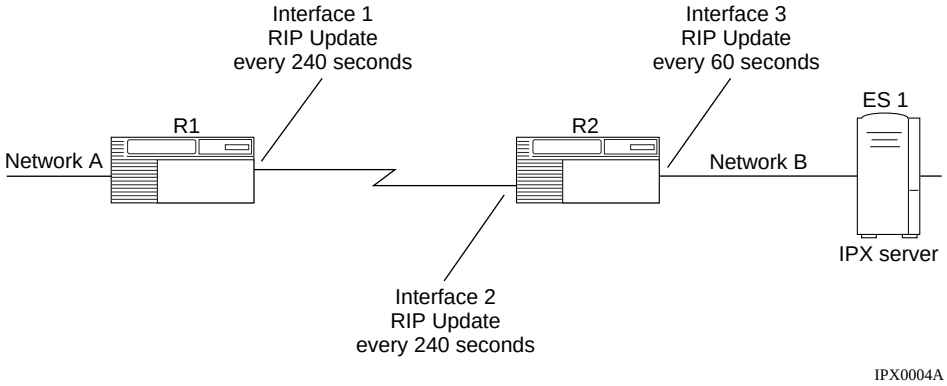

Figure 6-3. IPX Configurable RIP Timers

Taking into account the fact that IPX server ES1 (with an internal router) on network B expects periodic RIP advertisements every 60 seconds, router R2 continues to issue RIP advertisements out its LAN interface (interface 3) per the IPX specification, reconciling the fact that periodic RIP advertisements through interface 1 are received every 240 seconds.

Should you decide to disable the periodic transmission of RIP updates, RIP immediate (one-time) update packets still propagate through the network, in compliance with Novell standards.

The combination of the update interval and age multiplier should be the same for all systems on a network segment.

Note that increasing the value of the age multiplier can cause routes to take longer to age out; decreasing it could cause the router to age routes prematurely, if routing updates are missed.

Using the BCC

To configure RIP timers, you must configure the RIP update interval and age multiplier for information received in RIP periodic updates.

To specify a value for the RIP update interval, navigate to the RIP prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

update-interval *seconds*

seconds is an integer from 0 to 2,678,400 seconds.

For example, to set the update interval to 10,000 seconds, enter:

```
rip/00023456# update-interval 10000
```

To specify an age multiplier, navigate to the RIP prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

age-multiplier *integer*

integer is from 1 to 6.

For example, to set the age multiplier to 4, enter:

```
rip/00023456# age-multiplier 4
```

Using Site Manager

To configure RIP timers, complete the following tasks to configure the RIP update interval and age multiplier for information received in RIP periodic updates:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces.**	The IPX Interfaces window opens.
4. Choose **RIP.**	The IPX RIP Circuit window opens.
5. Set the following parameters: • **Update Interval** • **Age Multiplier** Click on **Help** or see the parameter descriptions on page B-37.	
6. Click on **OK**.	You return to the Configuration Manager window.

Adjusting the RIP Packet Size

By default the size of a RIP update packet is 432 bytes. You should leave the RIP packet size at the default value unless you have a reason for specifying a different packet size. If you must change the packet size, the packet size plus the IPX header (30 bytes) cannot exceed the MTU of the link.

Using the BCC

To specify the the RIP update packet size, navigate to the IPX RIP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

packet-size *bytes*

bytes is the size of the RIP packet in bytes.

For example, to set the IPX RIP update packet size to 500, enter:

```
rip/00023456# packet-size 500
```

Using Site Manager

To specify the the RIP update packet size, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **RIP.**	The IPX RIP Circuit window opens.
5. Set the **Packet Size** parameter. Click on **Help** or see the parameter description on page B-38.	
6. Click on **OK**.	You return to the Configuration Manager window.

Enabling Multicast Transmission of RIP Packets

By default, the IPX router broadcasts RIP packets. You can choose to enable multicast transmission of packets.

The multicast address causes the data link layer to issue a multicast packet on all active virtual circuits. The multicast address value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol.

You can use the default multicast address (0xFFFFFFFFFFFF), which causes the IPX router to send all multicast traffic through all logical connections associated with the IPX interface you are configuring. You can also specify a WAN multicast address to send all multicast traffic through the IPX interface you are configuring.

Using the BCC

To use multicasting, check that the router has enabled multicasting and then optionally specify a WAN multicast address.

By default, when you configure IPX on an interface, the router enables multicasting. To determine if the router has enabled multicasting, navigate to the IPX RIP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

multicast ?

If you previously disabled multicasting, reenable multicasting by entering:

multicast enabled

To specify a WAN multicast address, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

multicast-address *address*

address is a WAN multicast address.

For example, to enable multicasting and set the WAN multicast address to 0x00432567, enter:

```
rip 00023456# multicast enabled
rip 00023456# back
rip 00023456# multicast-address 0x00432567
```

To disable multicasting, navigate to the IPX RIP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

```
rip 00023456# multicast disabled
```

Using Site Manager

To enable multicasting and specify a WAN multicast address, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **RIP.**	The IPX RIP Circuit window opens.
5. Set the **Use Multicast** parameter. Click on **Help** or see the parameter descriptions on page B-38**.**	
6. Click on **OK**.	You return to the Configuration Manager window.
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **FR Multicast (hex)** parameter. Click on **Help** or see the parameter descriptions on page B-28**.**	
5. Click on **OK**.	You return to the Configuration Manager window.

Configuring Split Horizon

The split horizon algorithm is part of the Novell specification for the IPX protocol. Its purpose is to prevent circular routes and reduce network traffic. The Bay Networks implementation of split horizon excludes RIP and SAP updates learned from a neighbor when forwarding RIP and SAP updates to that neighbor. Split horizon is enabled by default for each interface. You can disable or reenable split horizon when you configure an IPX RIP circuit.

Fully Meshed Networks

A fully meshed network is a WAN in which all nodes have a logically direct connection to each other. Figure 6-4 shows a sample fully meshed network with split horizon enabled.

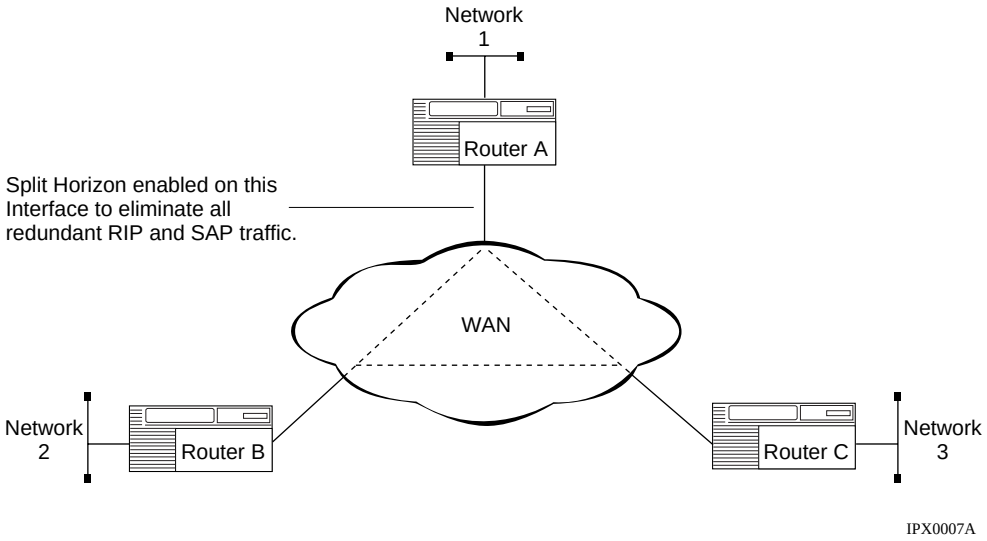

Figure 6-4. Split Horizon Enabled in a Fully Meshed Network

Non-Fully Meshed Networks

A non-fully meshed network is a WAN in which one or more nodes do not have logically direct connections to all other nodes. In a star or non-fully meshed frame relay or X.25 PDN topology, you may need to disable split horizon on certain interfaces so that the routers can learn about other networks.

Caution: Do not disable split horizon unless it is absolutely necessary. Doing so can result in a significant increase in network traffic.

Figure 6-5 shows a sample non-fully meshed network with split horizon disabled.

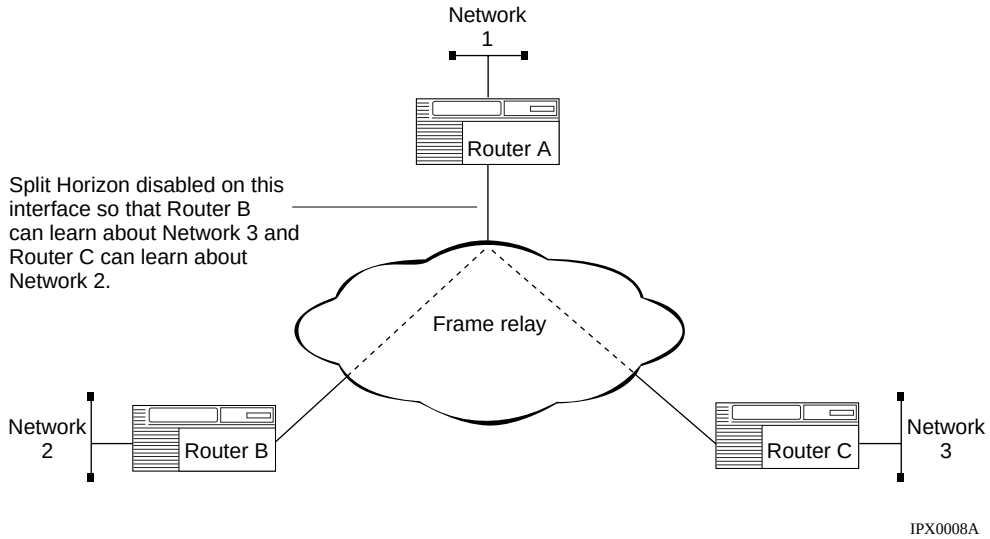

Figure 6-5. Split Horizon Disabled in a Non-Fully Meshed Network

If you disable IPX split horizon, IPX sends all router services over non-fully meshed frame relay and X.25 topologies. For example, as shown in Figure 6-5, router A propagates RIP and SAP packets pertaining to router B to router C, and vice versa. As a result, end stations on network 2 can learn about network 3, and end stations on network 3 can learn about network 2.

When you enable split horizon for an interface, routes learned on that interface are not advertised out that interface.

Using the BCC

To disable split horizon, navigate to the IPX RIP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

split-horizon disabled

To reenable split horizon, navigate to the IPX RIP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

split-horizon enabled

Using Site Manager

To disable or reenable split horizon, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **RIP.**	The IPX RIP Circuit window opens.
5. Set the **Split Horizon** parameter. Click on **Help** or see the parameter description on page B-39**.**	
6. Click on **OK**.	You return to the Configuration Manager window.

Updating Routers About a New or Failed Route

By default, when a circuit is added to a router or goes down on a router, the router immediately propagates this status change to other routers in the internetwork. When you disable this update mechanism, other routers learn about such changes only at the next periodic update interval.

Using the BCC

To specify that routers learn about new or failed routes only at the next periodic update interval, navigate to the IPX RIP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

triggered-update disabled

To specify that routers learn immediately about new or failed routes, navigate to the IPX RIP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

triggered-update enabled

Using Site Manager

To specify whether routers learn about new or failed routes immediately or only at the next periodic update interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **RIP.**	The IPX RIP Circuit window opens.
5. Set the **Immediate Update** parameter. Click on **Help** or see the parameter description on page B-39.	
6. Click on **OK**.	You return to the Configuration Manager window.

Advertising Default Routes in RIP Packets

A RIP packet does not normally include a default route that exists in the routing table. However, if a default route exists in the routing table, you can choose to advertise the default route, 0xFFFFFFE, in RIP packets on a circuit.

Using the BCC

To advertise default routes in RIP packets, navigate to the IPX RIP prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

default-supply enabled

If you do not want to advertise default routes in RIP packets, navigate to the IPX RIP prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

default-supply disabled

Using Site Manager

To specify whether a RIP interface advertises default routes in RIP packets, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces.**	The IPX Interfaces window opens.
4. Choose **RIP.**	The IPX RIP Circuit window opens.
5. Set the **Default Route Supply** parameter. Click on **Help** or see the parameter description on page B-40.	
6. Click on **OK**.	You return to the Configuration Manager window.

Accepting Default Route Information

By default, when a router receives a RIP packet that advertises a default route, the router does not store the default route in the routing table. You can choose to store the adcertised default route in the routing table.

Using the BCC

To specify that a RIP interface accepts the default route in RIP packets, navigate to the RIP prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

default-listen enabled

To specify that a RIP interface not accept the default route in RIP packets, navigate to the RIP prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

default-listen disabled

Using Site Manager

To specify whether a RIP interface accepts the default route in RIP packets, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces.**	The IPX Interfaces window opens.
4. Choose **RIP.**	The IPX RIP Circuit window opens.
5. Set the **Default Route Listen** parameter. Click on **Help** or see the parameter description on page B-40.	
6. Click on **OK**.	You return to the Configuration Manager window.

Customizing SAP Parameters

NetWare network services use the Service Advertising Protocol (SAP) to inform clients of their presence. NetWare services use the SAP identification broadcasting services to tell clients their name, type, and IPX address. The IPX address in a broadcast identifies a server's location in terms of network, host, and socket.

NetWare Directory Services (NDS) and SAP

Networks that implement NetWare 4.*x* use NetWare Directory Services (NDS) to advertise services. NDS is a globally distributed network database that replaces the bindery used in NetWare versions earlier than 4.0. Workstations locate services by querying an NDS server. NDS maintains information about all network resources (users, groups, servers, file volumes, printers, and so on) in a hierarchical tree structure. Network resources can be organized in the tree independent of their physical location. Thus, network users can access any network resource they have rights to without having to know the exact location of the resource.

With NDS, users no longer need to log in or attach to specific servers. Instead, users can log in to the network and get access to all authorized network resources. NDS is compatible with bindery-based versions of NetWare through the bindery emulation feature of NDS.

The NDS server distributes the service information using direct unicast-based protocols instead of using broadcast-based SAP. Therefore, the use of SAP in an NDS network is greatly reduced. Even in a network that includes only NetWare 4.0 servers, however, clients still use SAP to locate the nearest NDS server at startup.

SAP and the NetWare Bindery (NetWare 3.*x* and Earlier)

Novell IPX routers running NetWare versions earlier than 4.0 maintain a database called a *bindery.* The bindery includes information such as server type, IPX address, hop count, the interface to the server, a timer value for table entries, and a list of clients. If an entry in a bindery reaches its configured maximum age without being refreshed (timer resets to 0), the router deletes the entry from that bindery.

Bay Networks routers implement a similar structure (a global services table) for these services. Each time an IPX router receives a SAP packet, it compares the packet's contents to the contents of its SAP services table. If the SAP services table already contains information about a specific service, the router refreshes the age timer for that entry. If the SAP services table does *not* contain information about the service and a route exists to the service, the router adds a new entry to the services table and advertises the new service to all connected networks (except the one on which it was received).

Clients use SAP to request information about network services. Client information requests are nearest-service queries, which seek information about the closest service of a specified type. Every IPX server and IPX router on the internetwork learns about all other IPX servers and services through the propagation of bindery information or services table information.

By default, each SAP packet can contain up to seven service advertising updates. This number is configurable, but is constrained by the MTU of the outbound interface.

Disabling and Reenabling SAP

When you first configure SAP on an interface, it is automatically enabled. You can disable or reenable SAP.

Using the BCC

To disable SAP, navigate to the IPX SAP prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

state disabled

To enable SAP, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

state enabled

For example, to disable SAP on IPX interface 0x00023456, enter:

```
sap/00023456# state disabled
```

Using Site Manager

To disable or reenable SAP, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces.**	The IPX Interfaces window opens.
4. Choose **SAP.**	The IPX SAP Circuit window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page B-41.	
6. Click on **OK**.	You return to the Configuration Manager window.

Configuring SAP Timers

Configurable SAP timers are similar in function to configurable RIP timers. You configure the update interval by determining the timeout time, which consists of the frequency of SAP update transmissions and the holding multiplier for information received in SAP periodic updates. By default, the timeout time is three times the standard 60-second SAP advertisement update interval, or 180 seconds.

Configuring SAP timers can reduce IPX SAP overhead and enhance bandwidth availability. You can eliminate periodic SAP advertisements by setting configurable SAP timers to 0; thus, only triggered SAP updates are propagated.

To ensure proper SAP operation, all configurable SAP timers must be set at equal advertisement intervals on all Bay Networks router interfaces attached to common IPX network segments.

Note: Although you can set configurable SAP timers on any Bay Networks router interface, do not use them on LAN interfaces, because IPX servers do not currently support configurable SAP broadcast timers. As a result, IPX servers will purge SAP entries after 180 seconds if they have not received any updates within this time interval.

Using the BCC

To configure SAP timers, you must configure the SAP update interval and age multiplier for information received in SAP periodic updates.

To specify a value for the SAP update interval, navigate to the SAP prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

update-interval *seconds*

seconds is from 0 to 2,678,400 seconds.

For example, to set the update interval to 10,000 seconds, enter:

```
sap/00023456# update-interval 10000
```

To specify an age multiplier, navigate to the SAP prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

age-multiplier *integer*

integer is from 1 to 6.

For example, to set the age multiplier to 4, enter:

```
sap/00023456# age-multiplier 4
```

Using Site Manager

To configure SAP timers, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interface**.	The IPX Interfaces window opens.
4. Choose **SAP.**	The IPX SAP Circuit window opens.
5. Set the following parameters: • **Update Interval (sec)** • **Age Multiplier** Click on **Help** or see the parameter descriptions on page B-43.	
6. Click on **OK**.	You return to the Configuration Manager window.

Configuring a Default Route for SAP

A SAP advertisement can be learned from an interface when the network number advertised in the SAP advertisement is unreachable, but a default route is accessible from that interface. This feature gives you the option of making SAP entries available when the IPX default route is reachable.

If you enable SAP via default route, you enable IPX default routing globally for SAP advertisements and cause the router to accept a service if a direct or default router is known.

If you disable SAP via default route, the router accepts a service only if a direct route to the server advertising the service is known.

Note: Because his feature deviates from the IPX Default Route specification, enabling it may cause the interface to be incompatible with other router implementations.

Using the BCC

To enable SAP advertising via the default route, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

sap-via-default-route enabled

To disable SAP advertising via the default route, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

sap-via-default-route disabled

Using Site Manager

To enable or disable SAP advertising via the default route, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global.**	The edit IPX Global Parameters window opens.
4. Choose **Advanced**.	The Edit Advanced Global Parameters window opens.
5. Set the **SAP Via Default Route** parameter. Click on **Help** or see the parameter description on page B-20.	
6. Click on **OK**.	You return to the Configuration Manager window.

Enabling SAP Listen and Supply Functions

You can enable the listen and supply modes for each IPX SAP interface on the router. When you enable the listen mode, the IPX router listens for SAP periodic and triggered updates from neighboring networks and conveys received SAP service information to its internal SAP services table.

When you enable the supply function, the IPX router transmits all SAP periodic and triggered updates to routers in neighboring networks.

When you enable both the listen and supply modes, the IPX router performs both the listen and supply mode functions.

By default, the IPX router learns routes ands transmits updates to routers in adjacent networks.

Using the BCC

To specify that IPX not transmit periodic or triggered SAP updates, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

supply disabled

To specify that IPX transmits periodic or triggered SAP updates, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

supply enabled

For example, to specify that an IPX interface transmits triggered updates, enter:

```
sap/00023456# supply enabled
```

To specify that IPX not learn routes received in SAP updates from neighboring routers, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

listen disabled

To specify that IPX learns routes received in SAP updates from neighboring routers, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

listen enabled

For example, to specify that the IPX interface learns routes received in SAP updates from neighboring routers, enter:

```
sap/00023456# listen enabled
```

Using Site Manager

To specify whether IPX transmits or learns periodic or triggered SAP updates, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **SAP.**	The IPX SAP Circuit window opens.
5. Set the **Mode** parameter. Click on **Help** or see the parameter description on page B-42**.**	
6. Click on **OK**.	You return to the Configuration Manager window.

Determining the Pace of SAP Packets

The SAP pace determines the frequency, in packets per second, at which SAP sends packets on a circuit. By default, SAP sends 18 packets per second on a circuit.

You can specify a SAP pace from 0 to 1000 packets per second. If you enter a value of 0, there is no limit on the pace.

Using the BCC

To specify the SAP pace, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

pace *packets_per_second*

packets_per_second is the number of packets, from 0 to 1000, that SAP sends per second.

For example, to set the IPX SAP interface pace to 20 packets per seconds, enter:

`sap/00023456#` **pace 20**

Using Site Manager

To specify the SAP pace, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **SAP.**	The IPX SAP Circuit window opens.
5. Set the **Pace** parameter. Click on **Help** or see the parameter description on page B-42.	
6. Click on **OK**.	You return to the Configuration Manager window.

Adjusting the SAP Packet Size

By default the size of a SAP update packet is 480 bytes. You should accept the default SAP packet size unless you have a reason for specifying a different size packet. If you must change the packet size, the packet size plus the IPX header (30 bytes) cannot exceed the MTU of the link.

Using the BCC

To specify the the SAP update packet size, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

packet-size *bytes*

bytes is the size of the SAP packet.

For example, to set the IPX SAP update packet size to 500, enter:

`sap/00023456#` **packet-size 500**

Using Site Manager

To specify the packet size, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **SAP.**	The IPX SAP Circuit window opens.
5. Set the **Packet Size** parameter. Click on **Help** or see the parameter description on page B-44.	
6. Click on **OK**.	You return to the Configuration Manager window.

Responding to SAP GNS Requests

You can specify whether you want the router to respond to SAP get_nearest_server (GNS) requests.

By default, the router responds to SAP get_nearest_server requests. If you disabled split horizon, you may want to change this setting so that the router does not respond to SAP get_nearest_server requests.

Using the BCC

To specify that SAP not respond to get_nearest_server requests, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

nearest-server-reply disabled

To specify that SAP responds to get_nearest_server requests, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

nearest-server-reply enabled

Using Site Manager

To specify whether SAP responds to get_nearest_server requests, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **SAP.**	The IPX SAP Circuit window opens.
5. Set the **Nearest Server Reply** parameter. Click on **Help** or see the parameter description on page B-44.	
6. Click on **OK**.	You return to the Configuration Manager window.

Using a Multicast Address

By default, when you enable SAP on a router, the router uses a multicast address to send out SAP packets. You can change the setting to disable multicast transmission of SAP packets.

Using the BCC

To disable multicast transmission of SAP packets, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

multicast disabled

To enable multicast transmission of SAP packets, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

multicast enabled

Using Site Manager

To determine whether IPX allows multicast transmission of SAP packets, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **SAP.**	The IPX SAP Circuit window opens.
5. Set the **Use Multicast** parameter. Click on **Help** or see the parameter description on page B-44.	
6. Click on **OK**.	You return to the Configuration Manager window.

Saving the Full Service Name in SAP Packets

By default, a router saves all 48 bytes in the service name field of SAP packets. You can specify that a router should ignore all characters after the null character when a service field name is less than 48 bytes long.

Using the BCC

To cause the router to ignore all characters after the null character when a service field name is less than 48 bytes, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

save-full-name disabled

To cause the router to save all 48 bytes in the service name field of SAP packets, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

save-full-name enabled

Using Site Manager

To specify whether the router saves all 48 bytes in the service name field of SAP packets or ignores all characters after the null character when a service field name is less than 48 bytes, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **SAP.**	The IPX SAP Circuit window opens.
5. Set the **Save Full Name** parameter. Click on **Help** or see the parameter description on page B-45.	
6. Click on **OK**.	You return to the Configuration Manager window.

Transmitting and Receiving SAP Updates over the Same Interface

The split horizon algorithm is part of the Novell specification for the IPX protocol. Its purpose is to prevent circular routes and reduce network traffic. The Bay Networks implementation of split horizon excludes SAP updates learned from a neighbor when forwarding SAP updates to that neighbor. Split horizon is enabled by default for each interface. You can disable or reenable split horizon when you configure an IPX SAP circuit.

If you disable IPX split horizon, the router will transmit SAP updates received from one interface over that same interface.

See “Configuring Split Horizon” on page 6-49 for more information about split horizon.

Using the BCC

To disable split horizon, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

split-horizon disabled

To enable split horizon, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

split-horizon enabled

Using Site Manager

To disable or reenable split horizon, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **SAP.**	The IPX SAP Circuit window opens.
5. Set the **Split Horizon** parameter. Click on **Help** or see the parameter description on page B-45.	
6. Click on **OK**.	You return to the Configuration Manager window.

Updating Routers About a New or Failed Service

By default, the router performs immediate SAP updates so that when a change in status occurs for a circuit, the router immediately propagates this status change to other routers in the internetwork. When you disable immediate SAP updates, other routers learn about such changes only at the next periodic update interval.

Using the BCC

To specify that routers learn about new or failed services only at the next periodic update interval, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

triggered-update disabled

To specify that routers learn immediately about new or failed services, navigate to the IPX SAP interface prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

triggered-update enabled

Using Site Manager

To let routers know immediately about new or failed services, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **SAP.**	The IPX SAP Circuit window opens.
5. Set the **Immediate Update** parameter. Click on **Help** or see the parameter description on page B-46.	
6. Click on **OK**.	You return to the Configuration Manager window.

Using Static Services

When you statically configure NetWare services, the router learns about a NetWare service by means of the SAP information you enter. You can manually configure NetWare static services for each interface on a Bay Networks router.

When you configure static services on an interface, you can then use SAP filters to eliminate SAP announcements. The static service provides an alternative to broadcast SAP announcements across a WAN. The static service eliminates WAN traffic (and hence, the use of WAN bandwidth) associated with WAN SAP announcements.

Alternatively, you can disable SAP entirely on an individual interface or disable SAP immediate-update messages. For network topologies that include slower-speed WAN links, reducing the amount of WAN bandwidth otherwise needed for SAP announcements can be helpful.

Setting the Update Interval and Disabling Immediate Updates

To reduce traffic and disable immediate updates, you must configure the SAP update interval and determine whether you want to use immediate SAP updates.

A service sends an immediate update when one of the following conditions occurs:

- A service first comes up.
- A service changes.
- A service is no longer available.

Figure 6-6 shows a sample network configured to use static SAP services. If you want client 1 to have access only to file server 3, you configure file server 3 in the static SAP service table on router 2's interface. Then, to suppress any SAP broadcasts from router 1 and thus reduce bandwidth use, you can either turn off the SAP supply mode or disable SAP.

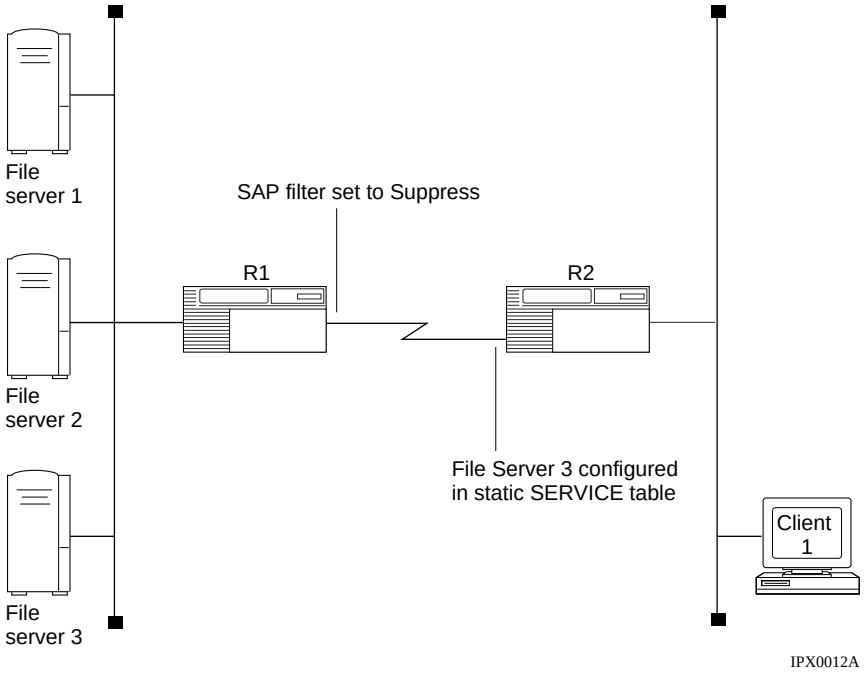

Figure 6-6. Static Service Network Configuration

Figure 6-7 shows another example, in which a SAP filter is configured on router R1, prohibiting periodic SAP advertisements and triggered SAP updates from being propagated over the wide area link. As a result, the services resident on server A and server B are not visible to networks C and D.

However, SAP services resident on servers A and B are manually entered into router R2's service table. This way, these servers are visible to IPX end stations on networks C and D (through periodic SAP advertisements, which are broadcast over router R2's LAN interfaces every 60 seconds, in conformance with IPX specifications). The key benefit in this example is that SAP overhead is eliminated over the WAN link.

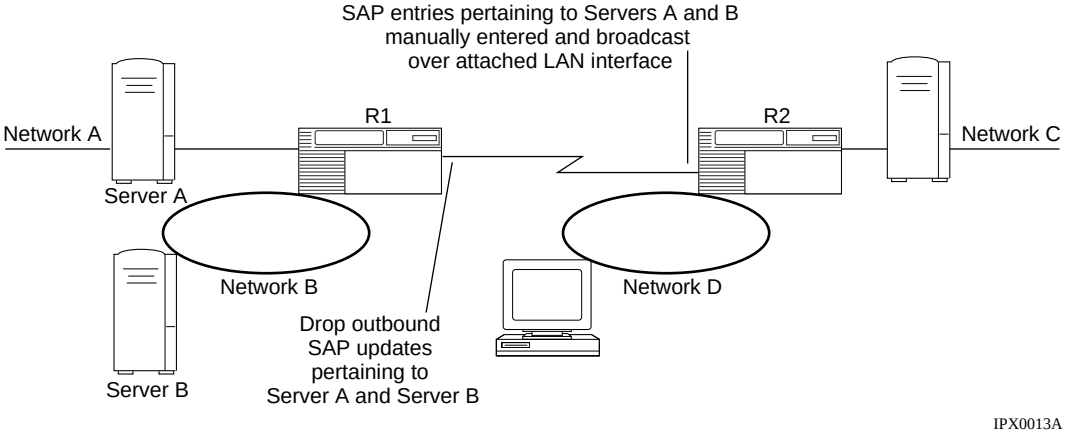

Figure 6-7. IPX SAP Filters Prohibiting SAP Broadcasts

Using the BCC

To specify a value for the SAP update interval, navigate to the SAP prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

update-interval *seconds*

seconds is from 0 to 2,678,400 seconds.

For example, to set the update interval to 10,000 seconds, enter:

`sap/00023456#` **update-interval 10000**

To disable immediate updates, navigate to the SAP prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

triggered-update disabled

Using Site Manager

To reduce traffic and disable immediate updates, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **SAP**.	The IPX SAP Circuit window opens.
5. Set the following parameters: • **Update Interval (sec)** • **Immediate Update** Click on **Help** or see the parameter descriptions on pages B-43 and B-46.	
6. Click on **OK**.	You return to the Configuration Manager window.

Note: Broadcast mechanisms, such as periodic RIP and SAP advertisements, can force dial-on-demand connections to be continuously established, preventing user-defined dial-on-demand expiration time limits from being reached. See the "Using Static Routing with Dial-on-Demand" on page 6-103 for more information.

Adding a Static Service

When adding a static service, you must supply :

- The name of the service you want to advertise. You can use the actual name of the server that the clients will attach to. Make this name meaningful to the network administrator. The name must be unique among all names assigned to IPX servers of the same type on the IPX internetwork. Once you supply a service name, you cannot change it. See the documentation that came with your NetWare operating system for guidelines on specifying a server name.
- The Novell service type you want to advertise from the associated IPX (LAN) interface. For a list of common service types, see Chapter D, "Common Service Types and Identifiers."

- Services that have valid network addresses. Valid network addresses are provided either by RIP or by statically configured routes. If you try to enter any services that have invalid network addresses in the router configuration, the router accepts the information, but the services are unreachable.

Using the BCC

To add a static service, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

static-service name *symbolic_name* **type** *<Novell_type>*

symbolic_name is the symbolic name of the service you want to advertise.

Novell_type is the Novell service type number in 4-digit hexadecimal format, including leading zeros.

For example, to add a static route with the name printer and the Novell type 0987:

`ipx/00023456#` **static-service name printer type 0987**

Using Site Manager

To add a static service, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Click on **Static/Filter Tables.**	The IPX Static Interface Tables Configuration window opens.
4. Click on **Static Serv.**	The IPX Static Services window opens.
5. Click on **Add**.	The

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Set the following parameters: • **Service Name** • **Service Type (hex)** • **Target network (hex)** • **Host Address (hex)** • **Socket (hex)** Click on **Help** or see the parameter descriptions beginning on page B-61.	
7. Click on **OK**.	You return to the Configuration Manager window.

Enabling Static Services

You enable a static service to restore client access to NetWare services configured earlier on the IPX interface. Disable a static service to make NetWare services configured earlier unavailable to clients.

Using the BCC

When you first configure a static service, by default it is enabled. To disable a static service, navigate to the IPX static service prompt (for example, **box; ethernet 2/1; ipx 00023456; static-service/00023456/printer/0987**) and enter:

state disabled

To reenable a static service, navigate to the IPX static service prompt (for example, **box; ethernet 2/1; ipx 00023456; static-service/00023456/printer/0987**) and enter:

state enabled

For example, to disable the static service named printer, enter:

```
static-service/00023456/printer/0987# state disabled
```

Using Site Manager

To disable or reenable a static service, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Click on **Static/Filter Tables.**	The IPX Static Interface Tables Configuration window opens.
4. Click on **Static Serv.**	The IPX Static Services window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page B-65.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Network Address of a Service

When you are using a static service, the network address for the service must exist as an entry in the IPX routing table. The router can learn the entry dynamically, or you can configure the entry as a static route. If you configure the entry as a static route, enter a network address of up to 8 hexadecimal characters.

Using the BCC

To specify the address for the static service, navigate to the IPX static service prompt (for example, **box; ethernet 2/1; ipx 00023456; static-service/ 00023456/printer/0987**) and enter:

network *address*

address is the network address for the service in hexadecimal notation.

For example, to specify 0x980976 as the address for a static service, enter:

```
static-service/00023456/printer/0987# network 0x980976
```

Using Site Manager

To specify the address for the static service, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Click on **Static/Filter Tables.**	The IPX Static Interface Tables Configuration window opens.
4. Click on **Static Serv.**	The IPX Static Services window opens.
5. Set the **Target Network (hex)** parameter. Click on **Help** or see the parameter description on page B-62.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Address of the Host That Provides a Service

You must specify the address of a remote IPX host (a NetWare server) that can provide local clients with specific NetWare services, such as file, print, gateway, or terminal server services. The remote IPX host address consists of a string of up to 12 hexadecimal characters (6 bytes).

Using the BCC

To specify the address of a remote IPX host, navigate to the IPX static service prompt (for example, **box; ethernet 2/1; ipx 00023456; static-service/ 00023456/printer/0987**) and enter:

host-address *address*

address is the address of a remote host in hexadecimal format.

For example, to specify 0x92416 as the address for a remote host, enter:

```
static-service/00023456/printer/0987# host-address 0x92416
```

Using Site Manager

To specify the address of a remote IPX host, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Click on **Static/Filter Tables.**	The IPX Static Interface Tables Configuration window opens.
4. Click on **Static Serv.**	The IPX Static Services window opens.
5. Set the **Host Number (hex)** parameter. Click on **Help** or see the parameter description on page B-65.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Socket Address of a Service

You must enter a socket address consisting of 4 hexadecimal characters when you are using a static service. Valid socket addresses have a value between 0x0001 and 0xFFFE.

Using the BCC

To enter a socket address for a static service, navigate to the IPX static service prompt (for example, **box; ethernet 2/1; ipx 00023456; static-service/ 00023456/printer/0987**) and enter:

socket *address*

address is a 4-digit hexadecimal socket address.

For example, to enter the socket address 0x1234, enter:

```
static-service/00023456/printer/0987# socket 0x1234
```

Using Site Manager

To specify the socket address, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Click on **Static/Filter Tables.**	The IPX Static Interface Tables Configuration window opens.
4. Click on **Static Serv.**	The IPX Static Services window opens.
5. Set the **Socket** parameter. Click on **Help** or see the parameter description on page B-66.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Hop Count

Enter the number of router hops that exist between a router and a specific remote Novell server or service. The number of router hops must be in the range of 1 to the number of maximum hops minus 1. The default number of hops is 1.

Using the BCC

To specify the number of hops, navigate to the IPX static service prompt (for example, **box; ethernet 2/1; ipx 00023456; static-service/00023456/printer/0987**) and enter:

hops *number_of_hops*

number_of_hops is in the range of 1 to the maximum number of hops minus 1.

For example, to set the maximum number of hops to 3, enter:

```
static-service/00023456/printer/0987# hops 3
```

Using Site Manager

To specify the number of hops, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Click on **Static/Filter Tables.**	The IPX Static Interface Tables Configuration window opens.
4. Click on **Static Serv.**	The IPX Static Services window opens.
5. Set the **Hop Count** parameter. Click on **Help** or see the parameter description on page B-66.	
6. Click on **OK**.	You return to the Configuration Manager window.

Customizing NetBIOS Static Routing

NetBIOS establishes sessions (logical connections) and allows for communication between PCs. You can map NetBIOS names to IPX destination networks by configuring a NetBIOS static route to a NetBIOS service name. The IPX router then converts the broadcast NetBIOS packets to directed broadcast NetBIOS packets, which are usually forwarded to all network interfaces on a single network. This reduces the amount of network traffic due to NetBIOS query requests; that is, broadcasts issued by NetBIOS clients seeking to find and establish sessions with specific NetBIOS applications over an IPX internetwork.

Besides minimizing NetBIOS broadcast traffic, using NetBIOS static routes allows a more precise logical partitioning of an IPX NetBIOS internetwork, enhancing internetwork security.

The Bay Networks IPX router software lets you specify whether:

- You want to direct a NetBIOS broadcast (type 20) packet through a network by configuring a static route only at the first router. Before the packet is directed out an interface, the router software overwrites the IPX destination address of the packet so that it can be routed to its destination. Because the IPX specification states that the network address of broadcast packets must be left unchanged, this option does not conform to Novell standards.
- You want the router to propagate a packet out all of its interfaces (in conformance with Novell standards).
- You want to direct a packet to its destination by configuring a static route for each hop in the network (in conformance with Novell standards).

In the NetWare environment, NetBIOS query requests are encapsulated within IPX packets. When a Bay Networks router receives an IPX packet containing a NetBIOS query request, it compares the NetBIOS name for which a connection is being requested to a statically configured NetBIOS name-to-IPX destination network table. If the requested NetBIOS name matches a table entry, the Bay Networks router forwards the query request packet out only one IPX interface toward the destination network. If a match does not exist, the router propagates the query request packet out all IPX interfaces, in conformance with the IPX specification.

In Figure 6-8, for example, when end system ES1 wants to find and establish a connection to a NetBIOS application on the IPX server ES2, it generates a query request broadcast packet. Router R1 receives the broadcast packet, consults its NetBIOS Name-to-IPX Destination Network table, finds that the NetBIOS application being requested is mapped to network B, and routes the packet out interface 1. Similarly, router R3 consults its NetBIOS Name-to-IPX Destination Network table upon receiving the NetBIOS query request, and routes the packet out its interface to network B.

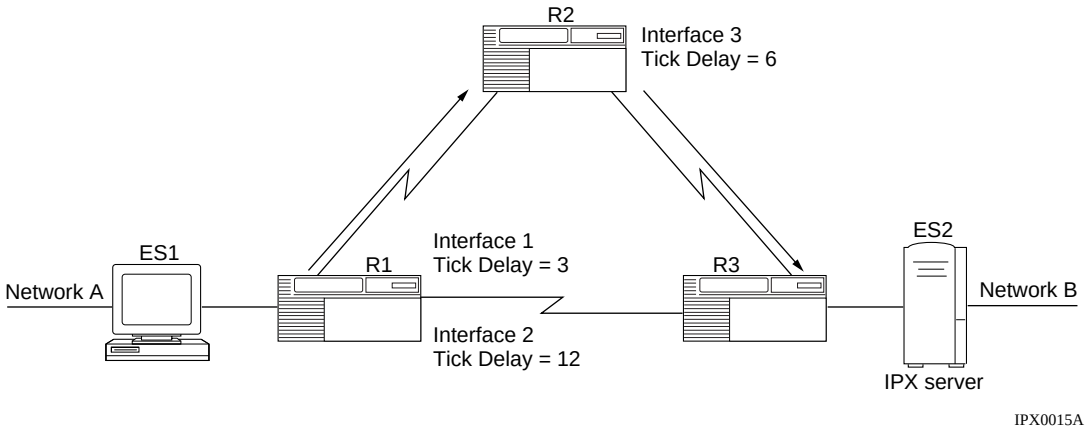

Figure 6-8. NetBIOS Static Routes

Each IPX router interface supports up to 50 NetBIOS static routes. Each NetBIOS static route specifies a NetBIOS resource name and a destination network where the resource resides.

Adding a NetBIOS Static Route

When you first add a NetBIOS static route, you must supply the name of the target server and the address of the target network. You cannot change the name of the target server or the address of the target network.

The target server name can consist of up to 16 alphanumeric characters. The name of a NetBIOS target server can include wildcard and pattern-matching characters, any printable character, including $, #, and so on. To specify a backslash, enter two backslashes (\\). You can also use the hexadecimal equivalent (*xx*) of any valid ASCII character. For example, you can specify \20 for space or \21 for ! (note that *xx* counts as one character). For a list of the wildcards and pattern-matching characters, see Table 6-1 on page 5-129.

When you send NETBIOS packets over a network, you must specify the address of a destination network that you want to receive NetBIOS broadcast packets destined for the specified target server. You can specify a target network address of up to 8 hexadecimal characters.

By default, the static route record is enabled (active) when you first add it.

Using the BCC

To add a NetBIOS static route, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

static-netbios-route name *name* **network** *address*

name is the symbolic name of the target server.

address is the address, in hexadecimal notation, of the target network.

For example, to add a NetBIOS static route on network address 0x00042567 and identify it as route6:

box# **static-netbios-route name route6 network 42567**

Using Site Manager

To add a NetBIOS static route, complete these tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **NetBIOS Static Routes**.	The IPX NetBIOS Static Routes window opens.
4. Click on **Add.**	The IPX NetBIOS Static Route Configuration window opens.
5. Set the following parameters. • **Target Server** • **Target Network (hex)** Click on **Help** or see the parameter descriptions beginning on page B-49.	
6. Click on **OK**.	You return to the Configuration Manager window.

Disabling and Reenabling the Static Route Record in the NetBIOS Routing Table

If you are sending NetBIOS packets over a network, you should enable this feature. By default, the router enables the static route record in the NetBIOS routing table.

Using the BCC

To disable the static route record in the NetBIOS routing table, navigate to the NetBIOS static route prompt (for example, **box; ipx; static-netbios-route/route6/00042567**) and enter:

state disabled

To reenable the static route record in the NetBIOS routing table, navigate to the NetBIOS static route prompt *(*for example, **box; ipx; static-netbios-route/route6/00042567***)* and enter:

state enabled

Using Site Manager

To disable or reenable the static route record, complete these tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **NetBIOS Static Routes**.	The IPX NetBIOS Static Routes window opens.
4. Set the **Enable** parameter. Click on **Help** or see the parameter description on page B-49.	
5. Click on **OK**.	You return to the Configuration Manager window.

Directing a NetBIOS Packet Using Nonstandard Static Routing

You can direct a NetBIOS packet through a network by configuring a NetBIOS static route on the first Bay Networks router to receive a NetBIOS broadcast packet. To do this, you must disable Novell certification conformance for all routers in the network.

To configure a router to propagate a packet out all its interfaces, you must enable Novell certification conformance for all routers in the network.

All NetBIOS packets sent from a client to the router must have a destination network value of 0, unless the packet passes a static route in the router. The router tests a packet against the static route table before it checks the packet's destination, thus allowing the router to accept packets that may not have a destination network of 0.

Caution: This method of defining IPX NetBIOS static routes is a nonstandard Bay Networks feature that may not be compatible with routers from other vendors. This method converts a NetBIOS broadcast packet to a NetBIOS directed broadcast packet, thereby eliminating the loop checking and path tracing that is usually done for NetBIOS broadcast packets. This may cause problems with applications that rely on those mechanisms.

When you configure a NetBIOS static route, the IPX router inserts the network number configured in the static route into the destination network number of the IPX packet.

When you configure NetBIOS static routes on an interface, the IPX router compares all IPX NetBIOS broadcast packets received on the interface with the boxwide NetBIOS static routes. If the NetBIOS destination name found in the packet matches an entry in the routing table, the NetBIOS packet is routed to the associated destination network. If no match is found, the IPX router treats the packet as specified by the NetBIOS Accept and NetBIOS Deliver parameters.

Using the BCC

By default, IPX enables Novell certification. To disable Novell certification, navigate to the global IPX prompt (for example **box; ipx**) and enter:

novell-certification-conformance disabled

To reenable Novell certification, navigate to the global IPX prompt (for example **box; ipx**) and enter:

novell-certification-conformance enabled

Using Site Manager

To enable or disable Novell certification conformance, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Global**.	The IPX Global Parameters window opens.
4. Click on **Advanced**.	The IPX Advanced Global Parameters window opens.
5. Set the **Novell Certification Conformance** parameter. Click on **Help** or see the parameter description on page B-21.	
6. Click on **OK**.	You return to the Configuration Manager window.

Directing a NetBIOS Packet Using Standard Static Routing

To configure NetBIOS static routes in conformance with Novell standards, you must configure a static route for each hop in the network. After you specify the static route to a NetBIOS name, the IPX router converts standard NetBIOS broadcast packets to NetBIOS *directed* broadcast packets.

- NetBIOS broadcast packets are sent to all accessible host IDs on *all* accessible IPX networks.
- NetBIOS directed broadcast packets are sent to all host IDs on a *single* IPX network.

Configuring NetBIOS Broadcast Filters

You can control the propagation of IPX NetBIOS broadcasts by configuring NetBIOS broadcast filters on an interface. This feature ensures that visibility to NetBIOS resources is limited to networks that need access to certain resources. This capability can enhance security and preserve bandwidth by controlling the flow of NetBIOS traffic.

You can configure an interface to either accept or not accept NetBIOS broadcasts from an attached network, and to deliver or not deliver NetBIOS broadcasts to a network. By default, both of these parameters are disabled.

Using the BCC

To specify that an interface accepts NetBIOS broadcasts from an attached network, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

netbios-accept enabled

To specify that an interface not accept NetBIOS broadcasts from an attached network, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

netbios-accept disabled

To specify that an interface delivers NetBIOS broadcasts from an attached network, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

netbios-deliver enabled

To specify that an interface not deliver NetBIOS broadcasts from an attached network, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

netbios-deliver disabled

Using Site Manager

To configure NetBIOS broadcast filters on an interface, complete these tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the following parameters: • **NetBIOS Accept** • **NetBIOS Deliver** Click on **Help** or see the parameter descriptions beginning on page B-27.	
5. Click on **OK**.	You return to the Configuration Manager window.

Note: The description that follows assumes that the NetBIOS destination name found in the packet does not match an entry in the NetBIOS static routing table.

When you enable an IPX interface to accept NetBIOS broadcasts, the IPX router accepts NetBIOS broadcast packets received on that interface. For example, in Figure 6-9, the IPX router accepts NetBIOS broadcast packets received only on interfaces 1 and 2.

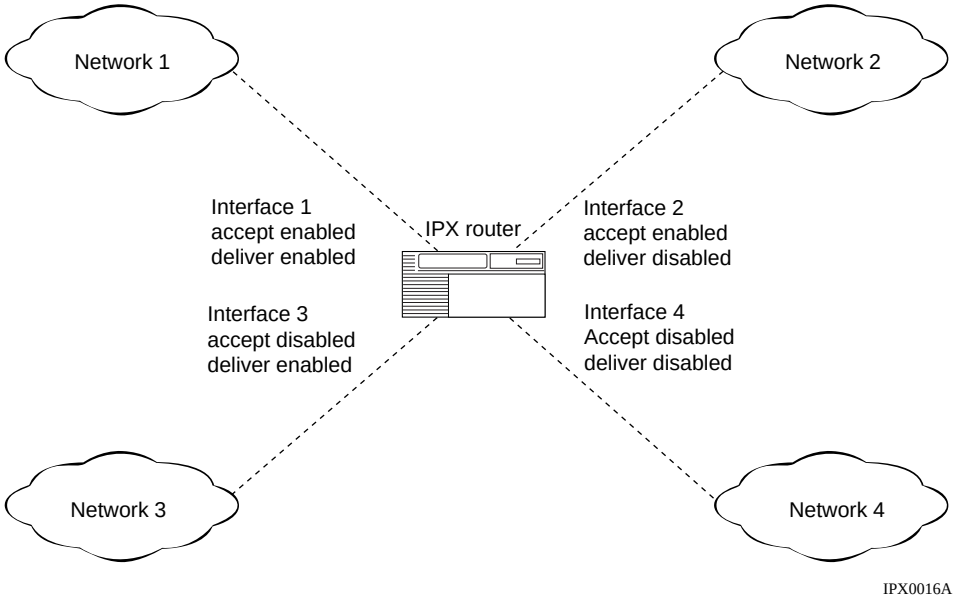

Figure 6-9. NetBIOS Packet Filtering

When you enable an IPX interface to accept NetBIOS broadcasts, the IPX router delivers NetBIOS broadcast packets that are routed to that interface. For example, in Figure 6-9, the IPX router delivers NetBIOS broadcast packets only to interfaces 1 and 3. The arrows in Figure 6-10 show the flow of packets in this same model.

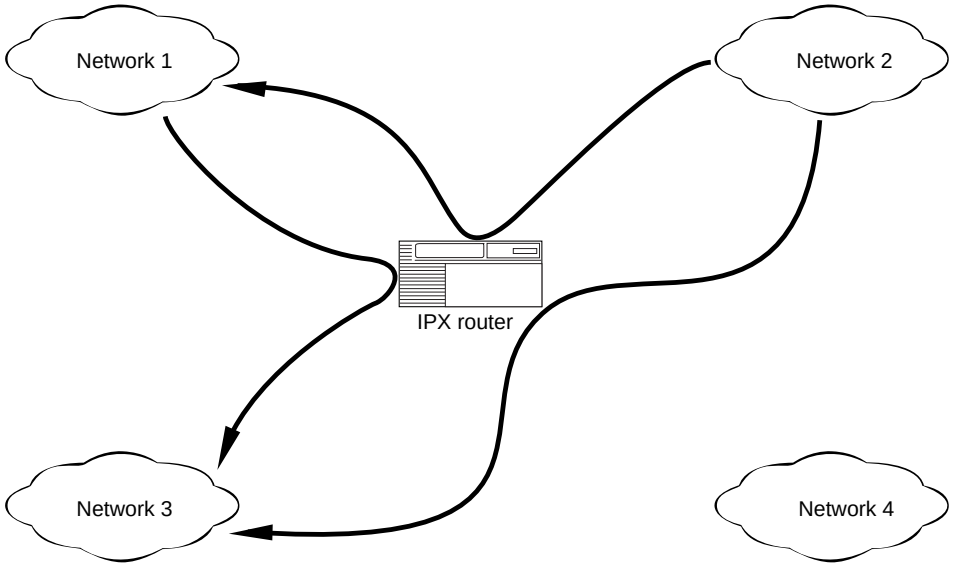

Figure 6-10. NetBIOS Packet Flow

You must enable an IPX interface to accept or deliver NetBIOS boradcasts for delivery of such packets to occur. For example, interface 1 can deliver only packets from interface 2 to network 1, because interface 2 is the only other interface that has been configured to accept NetBIOS broadcasts.

Thus, NetBIOS client applications on network 1 can initiate and establish sessions with NetBIOS server applications only on network 3. NetBIOS client applications on network 2 can initiate and establish sessions with NetBIOS server applications only on networks 1 and 3. Client applications on networks 3 and 4 cannot initiate any sessions with NetBIOS server applications via the IPX router.

As another example, in Figure 6-11, NetBIOS broadcasts from the end system ES1 on network A are *accepted* by router R1, but can be prohibited from network C by disabling the interface of router R1 connected to network C from delivering NetBIOS broadcasts. NetBIOS broadcasts will still be delivered to network B.

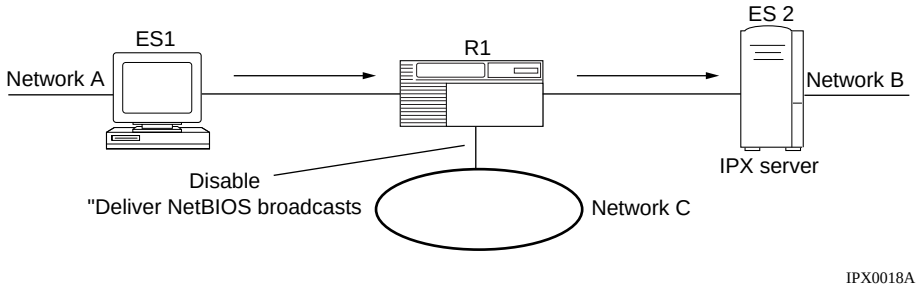

Figure 6-11. NetBIOS Broadcast Filtering

Configuring an Adjacent Host for an Interface

You can determine how the IPX router sends packets to a specific IPX host by configuring an IPX adjacent host. You can configure the adjacent host only if you are not using RIP on a circuit. Adjacent hosts typically use WAN media and do not require RIP.

Creating an Adjacent Host

To create an adjacent host on an IPX interface, you must specify, at a minimum, the host address of the adjacent host (up to 12 hexadecimal characters).

Using the BCC

To configure an adjacent host, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

adjacent-host host-address *address*

address is the address, in hexadecimal notation, of the adjacent host.

For example, the following command creates the adjacent host 000012345678::

`ipx/00023456#` **adjacent-host host-address 000012345678**

Using Site Manager

To create the adjacent host, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Adj. Hosts**.	The IPX Adjacent Hosts window opens.
5. Click on **Add**.	The IPX Adjacent Host Configuration window opens.
6. Set the **Host Address (hex)** parameter. Click on Help or see the parameter description on page B-51.	
7. Click on **OK**.	You return to the Configuration Manager window.

Disabling and Reenabling the Adjacent Host

You can set the state (active or inactive) of the adjacent host record in the IPX routing tables. By default, IPX activates the adjacent host record in the IPX routing tables.

Using the BCC

To disable the adjacent host, navigate to the adjacent host prompt (for example, **box;ethernet 2/1; ipx 00023456; adjacent-host host-address 000012345678**) and enter:

state disabled

To reenable the adjacent host, navigate to the adjacent host prompt (for example, **box; ethernet 2/1; ipx 00023456; adjacent-host host-address 000012345678**) and enter:

state enabled

For example, enter the following command to disable the adjacent host 000012345678::

```
adjacent-host/00023456/000012345678# state disabled
```

Using Site Manager

To specify the state of the adjacent host, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Adj. Hosts**.	The IPX Adjacent Hosts window opens.
5. Click on **Add**.	The IPX Adjacent Host Configuration window opens.
6. Set the **Enable** parameter. Click on **Help** or see the parameter description on page B-53.	
7. Click on **OK**.	You return to the Configuration Manager window.

Entering the ID of the Adjacent Host

If you are not using RIP on a circuit, supply the host ID of the adjacent host. You can enter a host ID of up to 12 hexadecimal characters. Once you supply the host ID of the adjacent host, you cannot change it.

Using the BCC

To configure an adjacent host and specify its address, navigate to the adjacent host prompt (for example, **box; ethernet 2/1;ipx 00023456; adjacent-host host-address 000012345678**) and enter:

host-address *address*

address is the address, in hexadecimal notation, of the adjacent host.

For example:

`ipx/00023456#` **host-address 000012345678**

Using Site Manager

To specify the host ID of the adjacent host, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Adj. Hosts**.	The IPX Adjacent Hosts window opens.
5. Click on **Add**.	The IPX Adjacent Host Configuration window opens.
6. Set the **Host Address** parameter. Click on **Help** or see the parameter description on page B-51.	
7. Click on **OK**.	You return to the Configuration Manager window.

Entering a WAN Address

If the interface you are configuring is on an ATM or SMDS network, supply a WAN address of up to 16 hexadecimal characters. If the interface is on a frame relay network, enter a WAN address or a decimal data link connection identifier number.

Using the BCC

To specify a WAN address, navigate to the adjacent host prompt (for example, **box; ethernet 2/1; ipx 00023456; adjacent-host host-address 000012345678**) and enter:

wan-number *number*

number is one of the following:

Number	Interface
Up to 16-character hexadecimal number	ATM or SMDS network
Decimal DLCI number	Frame relay network
X.121 address	X.25 switched virtual circuit
Logical channel number	X.25 permanent virtual circuit

Using Site Manager

To specify the WAN address, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Adj. Hosts**.	The IPX Adjacent Host window opens.
5. Click on **Add**.	The IPX Adjacent Hosts Configuration window opens.
6. Set the **Adjacent Host Address (hex)** parameter. Click on **Help** or see the parameter description on page B-51.	
7. Click on **OK**.	You return to the Configuration Manager window.

Creating a Frame Relay SVC to an Adjacent Host

You can create a frame relay SVC to an adjacent host. You must first enable frame relay SVC broadcasts and then identify the SVC.

To identify the SVC, you must supply:

- Hexadecimal address of the remote party
- Type of number used to establish an SVC to the adjacent host
- Type of adjacent host

Using the BCC

By default, the router enables frame relay SVC broadcasts on an IPX interface.

To disable frame relay SVC broadcasts, navigate to the IPX interface prompt (for example, **box; framerelay 3/1; ipx 00023456**) and enter:

svcbroadcast disabled

To enable frame relay SVC broadcasts, navigate to the IPX interface prompt (for example, **box; framerelay 3/1; ipx 00023456**) and enter:

svcbroadcast enabled

To identify the remote party, navigate to the adjacent host prompt (for example, **box; framerelay 3/1; ipx 00023456; adjacent-host host-address 000012345678**) and enter:

subaddress *address*

address is an 8-digit hexadecimal number.

For example, to set the subaddress to 0x67678934, enter:

```
adjacent-host/00023456/000012345678# subaddress 0x67678934
```

To identify the type of number used to establish an SVC to the adjacent host, navigate to the adjacent host prompt (for example, **box; framerelay 3/1; ipx 00023456; adjacent-host host-address 000012345678**) and enter:

type-of-number *option*

option is one of the following:

international
unknown

For example, to set the type of number to international, enter:

```
adjacent-host/00023456/000012345678# type-of-number unknown
```

To identify the type of adjacent host, navigate to the adjacent host prompt (for example, **box; framerelay 3/1; ipx 00023456; adjacent-host host-address 000012345678**) and enter:

type *host_type*

host-type is one of the following:

fre164
default
frx121
frdlci

For example, to set the type to fre164, enter:

```
adjacent-host/00023456/000012345678# type fre164
```

Using Site Manager

To create a frame relay SVC to an adjacent host, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **FR SVC Broadcast** parameter. Click on **Help** or see the parameter description on page B-30.	
5. Click on **OK**.	You return to the Configuration Manager window.
6. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
7. Choose **IPX**.	The IPX menu opens.
8. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
9. Choose **Adj. Hosts**.	The IPX Adjacent Host window opens.
10. Choose an adjacent host from the list.	The IPX Adjacent Hosts Configuration window opens.
11. Set the following parameters: • **Remote Party Sub-Address** • **Remote Party Type of Number** • **Adjacent Host Type** Click on **Help** or see the parameter descriptions beginning on page B-51.	
12. Click on **OK**.	You return to the Configuration Manager window.

Dial Services for IPX

A dial service provides access to a switched network by means of a dial-up line (also called a *switched line*). Dial-up lines are active only as needed -- that is, when there is data to send across the network, or when a dial-up line acts as a backup for a failed or congested leased line. Dial-up lines can be a cost-effective alternative to leased lines and packet networks, which are permanent connections and therefore available regardless of network traffic.

If you send a limited amount of data or your data transmission is intermittent, dial-up lines can be less expensive than leased lines, and they maximize network performance and flexibility.

The Bay Networks router provides three types of dial services: dial-on-demand, dial backup, and bandwidth-on-demand. Each dial service serves a different purpose:

- **Dial-on-demand** service reduces your line costs by establishing a connection between two devices only when there is data to send. You do not incur the cost of a leased line that is active regardless of data traffic.
- **Dial backup** service provides a backup circuit when a leased circuit fails. The backup circuit serves as an alternative path for data to reach the destination.
- **Bandwidth-on-demand** service provides up to 29 additional lines for a congested leased line, a dial-on-demand line, or a leased multilink bundle, providing a total of 30 lines for communication. The additional lines increase bandwidth for data traffic, improving communication and reducing network delays.

For more information about dial services, refer to *Configuring Dial Services*.

Using Dial-on-Demand Service

Dial-on-demand supports synchronous lines (RS-232, V.35, RS-422, and X.21) and ISDN interfaces. When dial-on-demand is configured, the router activates a dial-on-demand circuit for any one of the following reasons:

- The router has data to send across the circuit.

  When the router has data to transmit, it automatically selects one of the demand lines from the circuit's associated demand pool. As long as data is going across the line, the end-to-end connection remains active.

- You enabled a force dial to immediately activate a line and establish a connection.

The router brings down the circuit for any of these reasons:

- The configured inactivity time expires.
- You scheduled the circuit to come down.
- You enabled a forced takedown.

Figure 6-12 shows a dial-on-demand line connecting two routers. In this example, when the router has data to transmit across a demand circuit, or when you configure the router to bring up a demand circuit, the router instructs the dial device to establish a connection.

Note: Do not configure IPX adjacent hosts with dial-on-demand circuits.

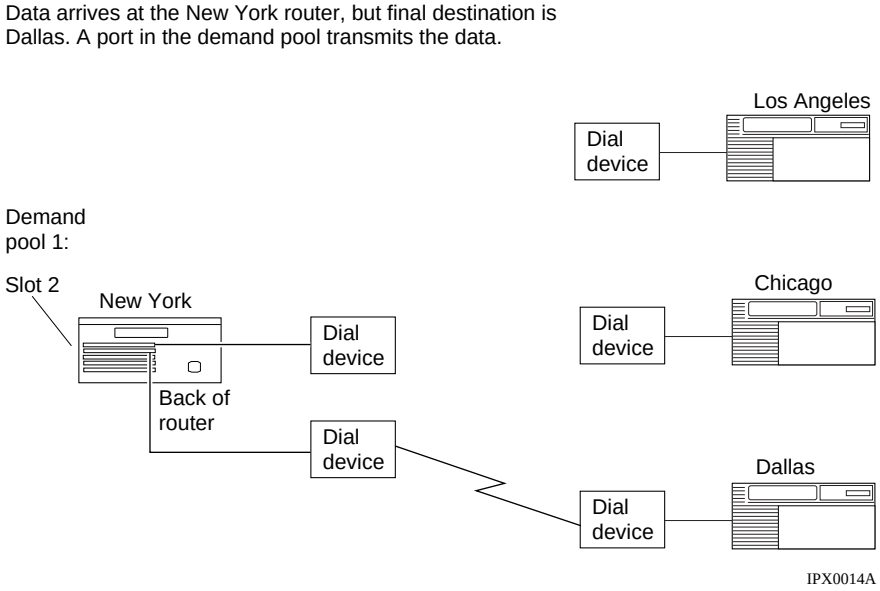

Figure 6-12. Dial-on-Demand Service

Using Static Routing with Dial-on-Demand

As part of its standard operation, IPX sends update packets to maintain routing tables and to gather information about network resources. For dial-on-demand, the frequency of these update packets forces the dial-up connection to remain up permanently, unless you configure a time of day to bring the connection down.

When you configure dial-on-demand circuits, you should disable broadcast messages. The router then uses static routes to determine the location of the destination network.

Tips for Using Dial-on-Demand with IPX

To optimize dial-on-demand with IPX:

- Turn off triggered updates.
- Set the periodic update interval to a large value; the line will be called only infrequently.
- Use service filtering, route filtering, or both.
- Use static routes and static services.
- Use the default route.
- Enable local watchdog acknowledgment (“spoofing”).
- Use traffic filters and protocol prioritization to prohibit routing updates and protocol-specific messages from keeping the circuit up unnecessarily (see *Configuring Traffic Filters and Protocol Prioritization* for details).

Enabling Local IPX Watchdog Acknowledgment

In a NetWare network, NetWare servers broadcast “watchdog” packets to verify that client nodes are still connected to the server. Watchdog packets are another type of data packet.

To maintain the connection, the client must respond to this watchdog message (essentially, responding to a poll). With a dial-up connection, this polling mechanism can mean dialing the phone line just to keep the server from bringing down the connection.

In addition, the bandwidth consumed by periodic RIP/SAP and watchdog broadcast packets can represent a significant portion of the total dial cost when charged on a per-packet basis. Depending on the network configuration and the application, this excessive broadcast activity can reduce application access performance.

To address this problem, Bay Networks routers can use local watchdog acknowledgment to improve the efficiency of IPX wide area links. This feature, also known as “watchdog spoofing,” lets Bay Networks routers locally respond to broadcast IPX watchdog packets on behalf of clients connected over dial-in connections.

Note: In a NetWare network, SPX keepalive packets are periodically transmitted to maintain SPX sessions between client and servers, initiating calls on dial-on-demand circuits. When you enable a local watchdog acknowledgment, the router also acknowledges these SPX keepalive packets.

Within an IPX network, servers rely on client watchdog acknowledgments to verify that client sessions are still active with the server. The router closest to the server responds on behalf of the client. As a result, NetWare servers may reach the maximum client sessions supported by the server, although not all clients are truly maintaining a session. This can happen if the client does not perform a standard closure of the session; for example, if the client PC is rebooted. You can avoid this potential problem by implementing NetWare’s auto logoff feature to ensure that client sessions are released when they are no longer in use.

Using the BCC

By default, the router does not use local watchdog acknowledgement.

To configure the router to use local watchdog acknowledgment, navigate to the IPXWAN prompt (for example, **box; serial 3/1; ppp; ipxwan 00055555**) and enter:

watchdog-spoofing enabled

To disable local watchdog acknowledgment, navigate to the IPXWAN prompt (for example, **box; serial 3/1; ppp; ipxwan 00055555**) and enter:

watchdog-spoofing disabled

For example, to configure an IPXWAN interface to use local watchdog acknowledgment, enter:

```
ipxwan/00055555# watchdog-spoofing enabled
```

Using Site Manager

To configure the router to use local watchdog acknowledgment, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Set the **IPX Watchdog Spoofing** parameter. Click on **Help** or see the parameter description on page B-29.	
5. Click on **OK**.	You return to the Configuration Manager window.

Configuring Dial-Optimized Routing for IPX

Dial-optimized routing lets you exchange IPX RIP/SAP routing updates only when a connection is active for data transmission. Limiting when the router can send updates reduces unnecessary connections and line costs.

For each dial-on-demand circuit, you can enable dial-optimized routing. If you enable dial-optimized routing, the router establishes a demand connection only for outbound data packets or through requests from the protocol. The presence of IPX RIP/SAP packets alone will not trigger a dial connection. If you disable dial-optimized routing, any packet can initiate demand connections.

After you enable dial-optimized routing on a dial-on-demand circuit, the router sends routing updates independent of data only as follows:

- The first time an IPX interface becomes active
- Triggered updates while the circuit is active
- Scheduled updates using a broadcast timer

You can use dial-optimized routing for IPX only after you enable it on a PPP dial-on-demand circuit. See *Configuring Dial Services* for instructions on how to enable dial-optimized routing.

Getting Optimum Performance Using IPX Dial-Optimized Routing

To use dial-optimized routing most effectively, Bay Networks recommends that you follow the practices described below:

1. **Set the inactivity mode to transmit only.**

   Any other setting causes the inactivity mode to reset when the receive end cannot filter serialization, watchdog, and keepalive packets for NORESET. These packets can keep the demand line active for long periods of time. For information about setting the inactivity mode, see *Configuring Dial Services.*

2. **Stop the router from clipping packets when an IPX DOR circuit comes up or changes state.**

   As IPX routes and services grow in number, IPX RIP and SAP packets may be clipped when an IPX DOR circuit comes up or changes state. To stop the clipping, reduce the value of the Pace parameter for RIP and SAP packets, or change the RIP/SAP packet size for the IPX DOR circuit. You should reduce the value of RIP/SAP Pace parameter for IPX DOR circuits to accommodate the number of IPX routes and services in the network.

3. **Reduce the frequency of bringing up the line for time synchronization packets.**

   No default priority queuing filters exist for IPX diagnostics packets or packets used in NDS time synchronization. You can configure a priority queueing filter to prevent IPX diagnostic packets from bringing up a demand line. However, because the Bay Networks IPX ping packet is a diagnostic packet, the filter will affect it as well.

   NDS time synchronization packets are treated as data packets. You can configure NetWare servers for larger polling intervals to reduce the frequency of bringing up the line for time synchronization packets.

Default IPX Dial-Optimized Routing Filters

Enabling IPX on a dial-optimized routing circuit creates several priority queuing (PQ) filters to reduce call initiation by various IPX packets. These filters prevent IPX watchdog packets, SPX keepalive packets, and IPX serialization packets from initiating calls or resetting the inactivity timer on IPX demand circuits.

Enabling or disabling dial-optimized routing on an IPX circuit affects the amount of time that RIP/SAP waits before sending out initial route information when the dial-on-demand route first becomes enabled, and the frequency of RIP/SAP updates.

Enabling or disabling dial-optimized routing on an IPX circuit changes the default values of the RIP and SAP delay periods to 120 seconds and the value of the RIP and SAP update intervals to 3600 seconds. If you enable dial optimized routing after configuring IPX on a circuit, you reset the Stabilization Timer Delay to 120 seconds and reset the RIP/SAP Update Interval to 3600 seconds. If you disable dial-optimized routing, reset the RIP/SAP delay period and RIP/SAP update interval to the default values.

Using the BCC

To set the maximum number of paths, you must configure:

- RIP/SAP delay period
- Update interval for RIP and/or SAP

To set the RIP/SAP delay period to the default value of 120 seconds, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

```
ipx/00023456# stabilization-timer 120
```

To change the RIP update interval period to 3600 seconds, navigate to the RIP prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**) and enter:

```
rip/00023456# update-interval 3600
```

To change the update interval period to 3600 seconds, navigate to the SAP prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**) and enter:

```
sap/00023456# update-interval 3600
```

Using Site Manager

To change the update interval period, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Interfaces**.	The IPX Interfaces window opens.
4. Choose **RIP**.	The IPX RIP Circuit window opens.
5. Set the following parameters: • **Timer Delay** • **Update Interval (sec)** Click on **Help** or see the parameter descriptions on pages B-29, B-37, and B-43.	
6. Click on **OK**.	You return to the Configuration Manager window.

Configuring RIP and SAP Broadcast Timers

A Bay Networks router running IPX lets you control the frequency of RIP and SAP update packet transmissions over both local and wide area links. RIP and SAP transmissions provide the following benefits:

- You spend less time manually configuring changes to static services and service routes across your network.
- You reduce the cost of administering Bay Networks routers installed across your network, compared to the cost of building static routes or static services tables.
- You allow a router to respond to changes in services and routes offered on the network.
- You enable users to have more accurate, up-to-date information on services and service routes offered on the network.

However, periodic RIP and SAP transmissions mean that:

- Less bandwidth is available for user data. Consequently, user data transmissions take longer, thereby increasing WAN line costs.
- You sacrifice some level of manual control over services and routes made available to network users. Your particular networking environment may require a higher degree of manual control over information about services and service routes offered to users on your network.

When you adjust the frequency of RIP and SAP update packet transmissions, the higher the number you specify, the less frequent the transmissions. If you specify zero, no periodic RIP or SAP updates are sent out the IPX interface of the router. However, RIP and SAP immediate (one-time) update packets still propagate through the network, in compliance with Novell standards. The default interval is 60 seconds.

Eliminating periodic RIP and SAP updates provides the following benefits:

- Reduced RIP and SAP overhead on your network
- Increased bandwidth available for user data
- Reduced WAN line costs for packet transmission
- Increased manual control over network services and routes

RIP and SAP timer settings should be the same on both sides of the WAN. Refer to the sections “Configuring RIP Timers” on page 6-43” and “Configuring SAP Timers” on page 6-58 for more detailed information.

Using Static Routes

A static route specifies a transmission path between networks.

The static route feature lets you manually define an IPX route to a destination network. Static routes specify the next hop in the transmission path a datagram must follow, based on the datagram’s destination address. You configure a static route to restrict the paths that packets can follow. A Bay Networks router running IPX lets you configure static routes on each logical IPX interface.

Using static routes is most valuable over wide area links, where bandwidth is at a premium. Static route support also enhances internetwork security, because it can brestrict traffic across specific IPX networks, protecting sensitive internetwork resources.

Static route support for IPX can do the following:

- Direct all IPX traffic not destined for this network to an adjacent host. The adjacent host may be the actual destination, or it may be the next hop to the eventual destination network. See “Configuring an Adjacent Host for an Interface” on page 6-92 for more information about adjacent hosts.
- Reduce routing traffic by disabling the RIP supply function on all or a subset of attached interfaces that are configured with static routes.
- Provide security by eliminating all dynamic routing capabilities and all RIP supply and listen activities over an IPX interface.

You should configure static routes and disable IPX RIP and SAP advertisements when implementing dial-on-demand routing over a wide area link. IPX RIP and SAP advertisements force dial-on-demand connections to be continuously established, which prevents user-defined dial-on-demand expiration time limits from being reached. See “Dial Services for IPX” on page 6-101 for details on using this feature.

Unlike routes learned through RIP, static routes remain in the route tables until you delete them. RIP routes have priority over static-learned routes if both routes have the same cost.

If you do not have the RIP listen functions enabled, the local network will not learn about new routes on the network, route changes, or deleted routes.

Static route support lets you identify the next interface and next router in the path toward a destination network. After you configure a static route for an interface, the router advertises that route in its usual RIP broadcasts.

For example, in Figure 6-13, to establish a static route between IPX network A and IPX network B, through interface 1 on router R1, a static route must be established from router R1 to router R2. The static route entry in router R1 directs any traffic destined for network B through interface 1 to router R2. In turn, the static route entry in router R2 directs any traffic destined for network B through interface 3 to router R3, and thus to network B.

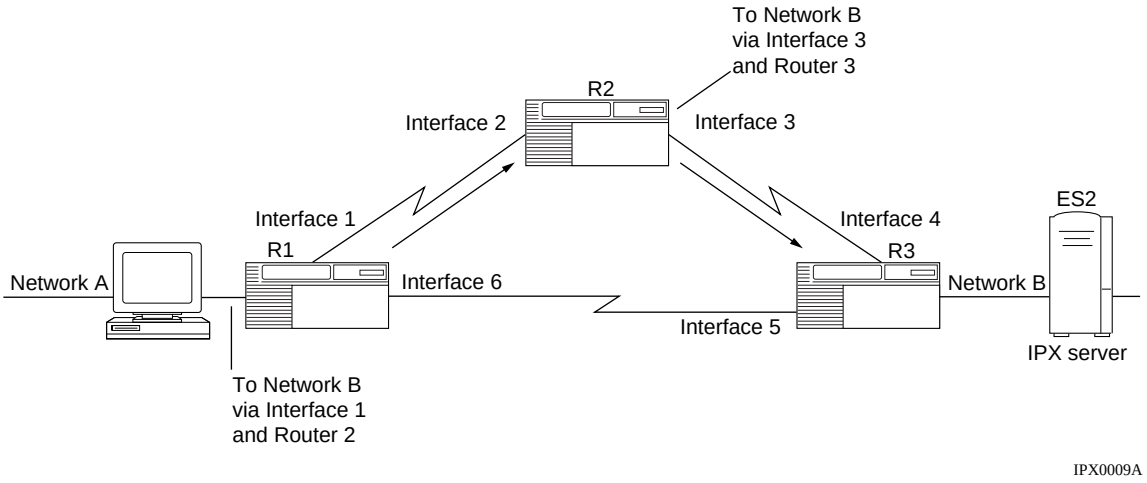

Figure 6-13. IPX Static Routes

RIP routes have priority over static-learned routes with the same cost, so if the connection between routers R1 and R3 has the same or greater cost, the packet will travel over the static route from router R1 to router R2 to router R3. If a connection used by the static route fails (and if router R1 has the listen function enabled), router R1 will learn of an alternative route between network A and network B and attempt to send the packet over that connection.

IPX static routes are user-specified routing table entries. Static routes, like routes learned through RIP, are maintained in the IPX routing table. Unlike routes learned through RIP, however, static routes do not expire. Static routes remain in the IPX routing table until they are reconfigured manually. Static routes are removed if the interface they are configured on goes down.

Note: You can send packets over a static route if you have mapped an IPX host address to a data link address in a Frame Relay, SMDS, or ATM network. If RIP is disabled on a WAN interface, before you configure a static route to an adjacent host, you must configure an adjacent host and edit the DLCI parameter.

Configuring a Static Route

To add a static route to an interface, you must specify the address of the network to which you want to configure the static route and the address of the next-hop host in the static routing path.

For the target network address, you can enter a network address of up to 8 hexadecimal characters or specify that the router use the default route 0xFFFFFFFE.

The next-hop host address consists of up to 12 hexadecimal characters. The next hop host is the host address of the down-stream router's IPX interface.

Note: You cannot change the next-hop host address once you have configured a static route.

Using the BCC

To add a static route, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**) and enter:

static-route target-network *net_address* **next-hop-host** *host_address*

net_address is up to 8 hexadecimal characters.

host_address is up to 12 hexadecimal characters.

For example, to configure a static route to network address 0x00004545 with the address of the next-hop host in the static routing path as 0x000008998987, enter:

```
ipx/00023456# static-route target-network  0x00004545 next-hop-host
0x000008998987
```

Using Site Manager

To specify the address of the next-hop host, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Static Route.**	The IPX Static Routes window opens.
5. Click on **Add.**	The IPX Static Route Configuration window opens.
6. Set the **Next Hop (hex)** parameter. Click on **Help** or see the parameter description on page B-57.	
7. Click on **OK**.	You return to the Configuration Manager window.

Changing the Target Network Address

If you are using the static route feature, you specified the target network address when you first configured to the static route. You cannot change the target network once you have configured the static route.

Using the BCC

To determine the target network address, navigate to the IPX static route prompt (for example, **box; ethernet/2/1; ipx 00023456; static-route 00023456/00054321/000000765432**) and enter:

target-network ?

Using Site Manager

To view the target network address, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Static Route.**	The IPX Static Routes window opens.
5. Click on **Add.**	The IPX Static Route Configuration window opens.
6. Set the **Target Network (hex)** parameter. Click on **Help** or see the parameter description on page B-56.	
7. Click on **OK**.	You return to the Configuration Manager window.

Entering the Hop Count

The IPX router uses a hop count when determining the best route for a datagram to follow. The hop count is also propagated through RIP. The default setting of 0 for static routes means “use the hop count associated with the interface.” You can accept the default value, zero, or enter a value from 1 to one less than the maximum number of hops.

Using the BCC

To specify the hop count, navigate to the IPX static route prompt (for example, **box; ethernet/2/1; ipx 00023456; static-route 00023456/00054321/ 000000765432**) and enter:

hops *count*

count is from 0 to one less than the maximum number of hops.

For example, to specify a hop count of 18, enter:

hops 18

Using Site Manager

To specify the hop count, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Static Route.**	The IPX Static Routes window opens.
5. Click on **Add.**	The IPX Static Route Configuration window opens.
6. Set the **Hop Count** parameter. Click on **Help** or see the parameter description on page B-57.	
7. Click on **OK**.	You return to the Configuration Manager window.

Setting the Timer Ticks

With the static route feature, you specify the number of 1/18th-second timer ticks required for an IPX datagram to traverse this static route. The IPX router uses tick cost when determining the best route for a datagram to follow. The tick cost is also propagated through RIP. The default setting of 0 for the tick cost of static routes means “use the tick count associated with the interface.” you can accept the default value, zero, or enter a value from 1 to the maximum positive integer.

Using the BCC

To specify the tick cost, navigate to the IPX static route prompt (for example, **box; ethernet/2/1; ipx 00023456; static-route 00023456/00054321/000000765432**) and enter:

ticks *cost*

cost is from 0 to one less than the maximum positive integer.

For example, to specify a cost of 20, enter:

ticks 20

Using Site Manager

To specify the number of timer ticks, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Static Route.**	The IPX Static Routes window opens.
5. Click on **Add.**	The IPX Static Route Configuration window opens.
6. Set the **Ticks** parameter. Click on **Help** or see the parameter description on page B-58.	
7. Click on **OK**.	You return to the Configuration Manager window.

Using RIP Route Filters

You can shield the view of networks from users on different network segments by configuring route filters. Route filters give you greater control over the routing of IPX packets from one area of an IPX internetwork to another. Using route filters helps maximize the use of the available bandwidth throughout the IPX internetwork, and helps improve network security by restricting a user's view of other networks.

You can configure inbound and outbound route filters on a per-interface basis, instructing the interface to advertise/accept or drop filtered RIP packets. The action parameter that you define for the filter determines whether the router advertises, accepts, or drops RIP packets from routers that match the filter criteria.

IPX route filters use the network number field in the IPX RIP packet. Network filtering is based on a two-part definition: filter ID and a corresponding mask. A route filter can be inbound, outbound, or both. You can define filters by network address, or by a range of network addresses.

The filter ID and the mask definition work together to determine which addresses are filtered on the interface. The character F in the mask definition requires an exact match with the corresponding character in the filter ID. The mask character 0(zero) matches any hexadecimal character. You can combine the F and 0 characters in any order in the mask to filter any combination of network and/or area addressing schemes used within the IPX internetwork.

For example, suppose you want to filter the range of network addresses from ABCD1200 to ABCD12FF. To do this, you would define:

- A filter ID of ABCD12FF
- A mask of FFFFFF00

In this example, the filter ID says, “This is the pattern to match.” The mask says, “The first six characters of the address must match the filter ID, but the last two characters are irrelevant.”

The IPX Route Filters window displays each route filter entry in the router configuration, as follows:

<rule_number>, <priority>, <circuit_index>, <filter_ID>, <filter_mask>

Once you have configured route filters, you can easily drop all routes to allow one or more specific routes. To drop all routes, apply a filter at a low priority. For example, in the IPX Route Filters window, enter the value 0xFFFFFFFF for the Target Network parameter, the value 0xFFFFFFFF for the Target Network Mask, and set the Action parameter to Suppress.

Add the filters you want by specifying higher priorities to advertise specific routes. For example, enter the value 0x3081be86 for the Target Network parameter, the value 0xFFFFFFFF for the Target Network Mask parameter, and set the Priority parameter to 1.

Using SAP Filters

An SAP filter is a pattern for matching a service name or service network. The router scans incoming and outgoing SAP packets to see whether certain fields in the packet match the filter. The type of filter (service name or service network) determines which fields the router examines. When you configure the filter, you can specify what the router does with the services in the packet when it finds a match.

You can create SAP filters on Bay Networks routers in your network to regulate both incoming and outgoing SAP advertisements. You can use SAP filters to control the size of resident SAP service tables and reduce bandwidth usage on your network due to SAP broadcast overhead. You can also create SAP filters as a security mechanism to restrict a user's view of services located elsewhere on the network.

Each SAP filter consists of a service name or network number, a service type, a priority, and a configurable action parameter. (You can also include wildcards or patterns to be matched. As a result, you can tailor SAP filters to your site requirements, improving network security by controlling access and preserving bandwidth by limiting the SAP packet traffic.

On a given interface, you can configure a filter as inbound, outbound, or both.

- *Inbound* filters affect only incoming SAP advertisements. The filter determines whether the Bay Networks router accepts or suppresses the service information from certain servers, based on the action that you specify.
- *Outbound* filters affect only outgoing SAP advertisements. The router either advertises or suppresses SAP information based on the action that you specify.
- *Both* applies the same filter pattern to both incoming and outgoing SAP advertisements.

Using the BCC

To specify that a SAP filter suppress incoming service information, navigate to the route filter prompt (for example, **box; ipx 00023456; route-filter 0x8888/0x2121**) and enter:

inbound disabled

To specify that a SAP filter accept incoming service information, navigate to the route filter prompt (for example, **box; ipx 00023456; route-filter 0x8888/0x2121**) and enter:

inbound enabled

To specify that a SAP filter disable outgoing SAP advertisements, navigate to the route filter prompt (for example, **box; ipx/00023456; route-filter 0x8888/0x2121**) and enter:

outbound disabled

To specify that a SAP filter enable outgoing SAP advertisements, navigate to the route filter prompt (for example, **box; ipx 00023456; route-filter 0x8888/0x2121**) and enter:

outbound enabled

Using Site Manager

To specify the filter mode, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Route Filter.**	The IPX Route Filters window opens.
5. Set the **Mode** parameter. Click on **Help** or see the parameter description on page B-71.	
6. Click on **OK**.	You return to the Configuration Manager window.

Figure 6-14 shows an example of SAP outbound filtering.

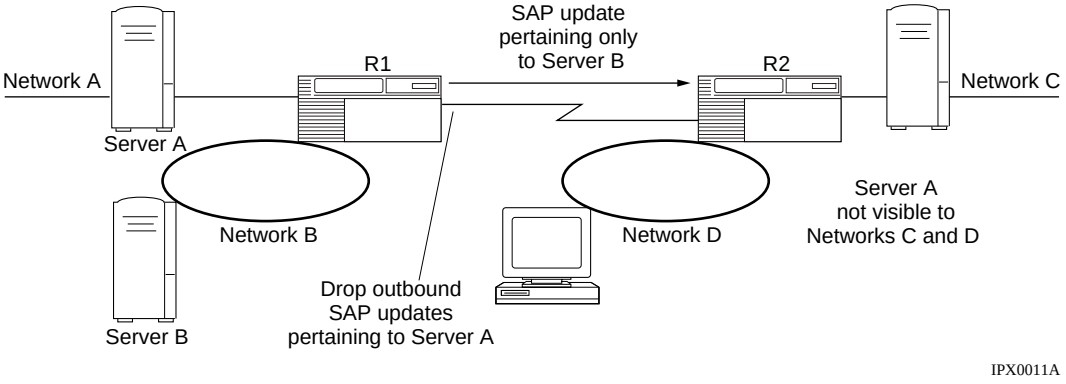

Figure 6-14. SAP Outbound Filtering

In this example, a SAP filter configured on router R1 prevents SAP advertisements and updates pertaining to server A from being propagated over the wide area link. As a result, server A is invisible to networks C and D. Information pertaining to server B, however, continues to be propagated over the WAN link.

Note: SAP filters restrict a user's view of network service information, but they do not prevent users from accessing services. If users have access to resources contained on an IPX network, they can also access all services within that network, regardless of whether a service has been filtered. The IPX router always updates its own SAP services table according to inbound SAP data.

You can configure SAP filters using the following levels:

- Individual servers
- Network level

Using SAP Filters at the Server Level

You can filter SAP service information pertaining to individual servers by editing server-level SAP filters.

At the service level, the filter matches a pattern that you specify (consisting of a service name pattern and a service type). The filter's Action parameter determines the action (Accept/Advertise or Suppress).

Note: You cannot change a SAP filter's actions once you have created a service name filter.

Using the BCC

To specify a SAP filter's action, navigate to the route filter prompt (for example, **box; ipx/00023456; route-filter 0x8888/0x2121**) and enter:

action *value*

value is one of the following:

Action	Meaning
Advertise	Enables the filter to allow advertisement or acceptance of routes that match the specified route filter criteria
Suppress	Causes the IPX router to drop advertisements that match the specified route filter criteria

For example, to enable the filter to accept routes that match the filter's criteria, enter:

```
route-filter 0x8888/0x2121# action advertise
```

Using Site Manager

To specify a SAP filter's action, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Net Filter.**	The IPX Service Network Filters window opens.
5. Set the **Action** parameter. Click on **Help** or see the parameter description on page B-80.	
6. Click on **OK**.	You return to the Configuration Manager window.

Using SAP Filters at the Network Level

You can filter service information pertaining to entire networks by editing network-level SAP filters.

At the network level, the filter matches a pattern that you specify (consisting of a service network number and a service type). The filter's action determines whether the router advertises or suppresses routes that match the filter's criteria.

Using the BCC

To determine the way a filter behaves at the service network level, you must specify the name and type of filter and then configure the action of the filter.

You specify the filter name when you initially configure a service network filter. Once you configure the filter, you cannot change the filter name. To specify the name of the filter, navigate to the IPX static service prompt (for example, **box; ethernet 2/1; ipx 00023456; static-service 00023456/printer/0987**) and enter:

name *name*

name is any valid alphanumeric filter name, or one containing wildcard characters or a pattern-matching regular expression.

For example, to set the filterr name to printer2, enter:

```
static-service/00023456/printer/0987# name printer2
```

You specify the type of the filter when you initially configure a service network filter. Once you configure the filter, you cannot change the filter type. To specify the filter type, navigate to the IPX static service prompt (for example, **box; ethernet 2/1; ipx 00023456; static-service 00023456/printer/0987**) and enter:

type *value*

value is any Novell filter type number in hexadecimal format.

For example, to set the server type to 0x2121, enter:

```
static-service/00023456/printer/0987# type 0x2121
```

To configure a filter's action, navigate to the route filter prompt (for example, **box; ipx/00023456; route-filter 0x8888/0x2121**) and enter:

action *type*

type is one of the following:

Action	Meaning
Advertise	Enables the filter to allow advertisement or acceptance of routes that match the specified route filter criteria
Suppress	Causes the IPX router to drop advertisements that match the specified route filter criteria

Using Site Manager

To specify a filter's action at the service network level, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Name Filter.**	The IPX Service Name Filters window opens.
5. Set the following parameters: • **Action** • **Target Service Name** • **Target Service Type (hex)** Click on **Help** or see the parameter descriptions on pages B-85 and B-87.	
6. Click on **OK**.	You return to the Configuration Manager window.

The IPX router with an outbound filter configured on an interface includes information about a service in a SAP packet if either of the following is true:

- The router finds a match between an outbound filter's contents and the service in its SAP services table, and the filter action is Advertise/Accept.
- The router does not find an outbound filter that matches the service in its SAP services table.

The IPX router excludes information about a service from a SAP packet only if it finds a match between an inbound filter's contents and the contents of its SAP services table, and the filter action is Suppress.

Similarly, the IPX router accepts information about a service in a SAP packet if either of the following is true:

- The router finds a match between an inbound filter's contents and the service in the SAP packet, and the filter action is Advertise/Accept.
- The router does not find an inbound filter that matches the service in the SAP packet.

Using Wildcards and Pattern Matching with SAP Filters

Wildcards and pattern matching are shortcut techniques for setting up SAP filters. Wildcards are characters that match zero or more instances of any valid character. In other words, a wildcard in a filter matches any allowable characters, depending on which wildcard you specify. Pattern matching lets you selectively filter by named entities. The following sections describe each of these techniques.

Using Wildcards with SAP Filters

Using wildcards in SAP filters, you can configure a single SAP filter to match a set of services. When you use wildcards, you can configure the filter based on the service name, which lets you configure a SAP filter based on the characters represented in the service name field of an IPX SAP packet. The service name field contains the 48-byte character string name that is assigned to a NetWare server. The service name, in combination with the service type, uniquely identifies a service on the internetwork. You can use a wildcard SAP filter configured using the service name field to restrict users' view of services that reside on a group of servers that use a common naming convention.

The wildcard characters are:

- An asterisk (*) matches any number of instances (zero or more) of the previous character.
- A period (•) matches any *single* character.

For example, an organization has 10 servers within its network, each providing a variety of different services. Five of the servers have names that begin with the letter **p**; the other servers have names that start with a different character. You could then define a single SAP filter **p•*** that would filter all SAP information for all five servers whose server name begins with the letter **p**.

Similarly, a SAP filter defined as p•int would match the server names **print**, **point**, and **paint**, but not the server name **poing**, because the wildcard character • matches only a single character in the same position in the string that makes up the server name.

Using Pattern Matching with SAP Filters

You can also filter SAP packets by matching a filter pattern that you define as a *regular expression*, using the characters shown in Table 6-1. The software compares this regular expression against a service name and indicates whether it finds a match. Functionally, pattern matching on SAP filters is similar to the UNIX **grep** command.

Table 6-1. Characters in SAP Pattern-Matching Filters

Filter Character	Function
C	Matches any character, except those listed below. An ordinary character (such as a, b, 7, or q) matches only itself.
\ (Backslash)	The backslash (\) is the escape character. Use this to match a character that would otherwise have special meaning to the software. The special characters that must be preceded by a backslash to match themselves are: **** (backslash) **.** (period or dot) **[** (left bracket) **?** (question mark) ***** (asterisk) **{** (left brace) **(** (left parenthesis) **)** (right parenthesis) **|** (vertical bar) **$** (currency symbol) Must be quoted only when it is the last character to be matched. Any other quoted character following a backslash matches itself. For example, to match a backslash (\) in a string, include the following in the filter expression: \\
. (Dot or period)	Matches a single character Example: **SERVER.** Matches: SERVER1 and SERVERA Does not match: SERVER12 or SERVER

(continued)

Table 6-1. Characters in SAP Pattern-Matching Filters *(continued)*

Filter Character	Function
[c...]	As the rightmost element in a string, this element tells the filter to match *any one* of the characters enclosed in the brackets. To use a right bracket (]) as one of the characters to be matched, make it the first character in the string. The expression: [ ]abc] matches any of the characters:], a, b, or c.
[^c...]	When a caret is the first character of the enclosed string, the filter expression matches any character *except* those in the remainder of the string. For example, the expression [^45678] matches any character except 4, 5, 6, 7, or 8. To include a right bracket (]) in the string of filtered characters, place it directly after the caret. For example, the expression [^] abc] matches every character except], a, b, or c.
[l-r]	The hyphen between two characters indicates a range of consecutive ASCII characters to match. This bracketed string of characters is known as a *character class*. For example, the range: [0-9] is equivalent to the string: [0123456789] The hyphen (-) is treated as an ordinary character if it occurs first (or first after an initial ^ character) or last in a string.

You can also construct longer filters by combining (that is, concatenating) these single-character regular expressions using the rules and operators listed in Table 6-2. A filter made up of a concatenation of regular expressions matches a concatenation of text strings, each of which is a match for a successive regular expression in the search pattern.

Table 6-2. Concatenation Rules and Operators

Rule/Operator	Interpretation
? (Question mark)	A single-expression regular expression followed by a question mark (?) matches *zero or exactly one* occurrence of that single-character regular expression. For example, [a-z]**?** matches any string of either zero lowercase letters or exactly one lowercase letter. Example: **SERVER?** Matches: SERVER1 and SERVER Does not match: SERVER12 or SERVER123
***** (Asterisk)	A single-expression regular expression followed by an asterisk (*) matches zero or more occurrences of that single-character regular expression. For example, [a-z]***** matches any string of zero or more lowercase letters. Example: **SERVER*** Matches: SERVER123 and SERVER Does not match: ADMIN123 or PS_SERVER
+ (Plus sign)	A single-expression regular expression followed by a plus sign (+) matches one or more occurrences of that single-character regular expression. For example, [a-z]+ matches any string with one or more lowercase letters. Example: **SERVER+** Matches: SERVER12 and SERVERA Does not match: SERVER or ADMIN123
{m} **{m,}** **{m,n}** (where m and n are integers)	A one-character regular expression followed by {m}, {m,}, or {m,n} is a regular expression that matches a range of occurrences of the one-character regular expression. The values *m* and *n* must be non-negative integers less than 255. The symbols in braces mean the following: {m} matches *exactly* m occurrences. {m,} matches *at least* m occurrences. {m,n} matches *any number* of occurrences between m and n. Whenever a choice exists, the regular expression matches as many occurrences as possible. For example, the **?** operator is equivalent to {0,1}, the ***** operator is equivalent to {0,}, and the **+** operator is equivalent to {1,}.

(continued)

Table 6-2. Concatenation Rules and Operators *(continued)*

Rule/Operator	Interpretation
Use the following operators to construct regular expressions from more-than-single-character regular expressions.	
(...) (Regular expressions enclosed in parentheses)	A regular expression enclosed within parentheses matches whatever the unadorned regular expression matches. You use parentheses to group a series of regular expressions that you want to treat as a single-character regular expression. For example, the regular expression **0[Xx]?** matches a 0 that may or may not be followed by one X or x, while the regular expression **(0[Xx])?** matches nothing, the string "0X," or the string "0x." You can have up to nine such substrings in a regular expression, and you can nest parentheses.
| (Vertical bar)	Two regular expressions separated by the vertical bar (|) match either a match for the first or a match for the second. These two regular expressions are the longest that can be created subject to parentheses grouping. For example, these regular expressions are grouped as follows: and|or = and | or and*|o+r = and* | o+r a(nd|o)r = a, plus either nd or o, plus r Example: **SERVER(8FS|1FS)** Matches: SERVER8FS and SERVER1FS Does not match: SERVER or SERVER5FS
[ ] (Square brackets)	Matches any single character in the bracketed set. Example: **SERVER[123]** Matches: SERVER1 and SERVER3 Does not match: SERVER123 or SERVER23

Service name filters take precedence over service network filters. Both service name and service network filters have an associated priority, with smaller values denoting a higher priority. Matching is performed by first checking all service name filters in order by priority. If a match is not found, then the service network filters are checked in order by priority.

For example, you may want to advertise from an IPX interface only one type of service (type 4) belonging to a particular server (server 1). You can configure:

- A service name SAP filter with a target service name of server 1, a service type of 4, and an action to advertise.
- A service network filter with a target network of 0xFFFFFFFF, a type of 0xFFFF, and an action to suppress. (This service network filter prevents all other services from being advertised from the interface.)

Using similar specifications and an action to suppress, you could exclude from an IPX interface a type of service from a particular server.

Note: The order in which you create SAP filters does not affect filter precedence.

Example of Using SAP Filters

The following example describes a situation in which you want to configure SAP filters. An office complex contains three buildings. The employees in each building use only the print services within their own building and have no need to send files to printers outside their building. To conserve bandwidth, you could configure a SAP filter that suppresses print server advertisements on the interfaces of the routers that connect the three buildings.

To suppress print server advertisements, configure a service network filter on the interfaces of the routers that connect the three buildings and suppress the advertisement of Server Type 0x0047 (print server) for all networks (0xFFFFFFFF). Refer to Appendix D, “Common Service Types and Identifiers” for a list of common service types.

The IPX Service Network Filters window displays each service network filter entry in the router configuration, as follows:

<filter/rule_no.>, <filter_priority>, <circuit_number>, <target_network_number>, <target_network_mask>, <target_service_type>

After you configure SAP filters, you can easily drop all services to allow one or more specific services. To drop all services, apply a filter at a low priority.

To configure filters of this type:

Using Site Manager, open the IPX Service Network Filters window, and for the Target Network (hex) and Target Network Mask (hex) parameters, enter 0xFFFFFFFF (see page B-78). Then set the Action parameter to Suppress (see page B-80).

Add the filters you want by specifying higher priorities to advertise specific services.

Example

For the target network, enter the value 0x3081be86, for the target network mask, enter the value 0xFFFFFFFF, and for the target service type, enter the value 0x0004, and set the filter priority to 1.

Configuring Service Name Filters

The service name filters function lets you reduce network traffic by configuring service name filters.

Enabling an IPX Service Name Filter

If you are configuring service name filters, you must activate the service name filter for each interface.

By default, the service name filter is active on an interface. You can disable the service name filter if you do not want to use this feature.

Using the BCC

To enable the service name filters, you must first configure a service name filter. To configure a service name filter, navigate to the IPX interface prompt (for example, (**box; ethernet 2/1; ipx 0x00023456**) and enter:

server-name-filter name *name*

name is any valid alphanumeric server name.

For example, to set the service name to Hoboken, enter:

```
ipx/00023456# server-name-filter name Hoboken
```

By default, when you activate the service name filters, the router enables the filter feature. To disable the service name filters feature, navigate to the service name filter prompt, (for example, **box; ethernet 2/1; ipx 0x00023456; server-name-filter 00023456/myname**) and enter:

state disabled

To reenable the service name filters, navigate to the service name filter prompt, (for example, **box; ethernet 2/1; ipx 0x00023456; server-name-filter 00023456/myname**) and enter:

state enabled

Using Site Manager

To activate the service name filters feature, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Name Filter.**	The IPX Service Name Filters window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page B-84.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Target Server Name

Enter the name of the server to which you are applying the server-level SAP filter, or enter a filter containing a wildcard or a pattern (regular expression) to be matched. The server name or filter pattern can consist of up to 48 alphanumeric characters.

You can specify any valid alphanumeric server name, or one containing wildcard characters or a pattern-matching regular expression. See “Using Wildcards and Pattern Matching with SAP Filters” on page 6-127 for lists of these characters.

Using the BCC

To specify the service name or filter type, navigate to the server name filter prompt (for example, **box; ethernet 2/1; ipx 0x00023456; server-name-filter 00023456/myname**) and enter:

name *name*

name is any valid alphanumeric server name.

For example, to set the service name to Hoboken, enter:

```
server-name-filter/00023456/myname# name Hoboken
```

Using Site Manager

To specify the service name or filter type, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Name Filter.**	The IPX Service Name Filters window opens.
5. Set the **Target Server** parameter. Click on **Help** or see the parameter description on page B-85.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Target Service Type

If you are using a service name filter, you must specify the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment. To specify the server type, enter the server type number in 4-digit hexadecimal format, making sure to include leading zeros. For all types, enter a value of 0xFFFF. See Appendix D, "Common Service Types and Identifiers" for a list of common service types.

Using the BCC

To specify the type of service, navigate to the service name filter prompt (for example, **box; ethernet 2/1; ipx 0x00023456; server-name-filter 00023456/myname**) and enter:

type *server_type*

server_type is any valid Novell server type in hexadecimal format.

For example, to set the server type to 0x0987, enter:

```
server-name-filter/00023456/myname# type 0x0987
```

Using Site Manager

To specify the type of server, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Name Filter.**	The IPX Service Name Filters window opens.
5. Set the **Target Service Type (hex)** parameter. Click on **Help** or see the parameter description on page B-85.	
6. Click on **OK**.	You return to the Configuration Manager window.

Setting the Filter Priority

Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. You can specify a priority in the range of 0 to the maximum positive integer. Lower values indicate higher priorities. The highest priority is zero.

Using the BCC

To specify a filter's priority, navigate to the service name filter prompt (for example, **box; ethernet 2/1; ipx 0x00023456; server-name-filter 00023456/myname**) and enter:

priority *value*

value is a decimal value from 0 to the maximum positive integer.

For example, to set the priority to 12, enter:

```
server-name-filter/00023456/myname# priority 12
```

Using Site Manager

To specify a filter's priority, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Name Filter.**	The IPX Service Name Filters window opens.
5. Set the **Filter Priority** parameter. Click on **Help** or see the parameter description on page B-86.	
6. Click on **OK**.	You return to the Configuration Manager window.

Applying Filters to Inbound or Outbound Packets

You can apply the service name filter to inbound packets, outbound packets, or both. By default, the filter is applied to SAP packets advertised by the specified interface. If you want to apply the filter to SAP packets coming into this interface, specify inbound. If you want to filter both incoming and outgoing packets, specify both.

Using the BCC

By default, the router does not apply service name filters to inbound packets. To apply the service name filter to inbound packets, navigate to the service name filter prompt (for example, **box; ethernet 2/1; ipx 0x00023456; server-name-filter 00023456/myname**) and enter:

inbound enabled

If you do not want to apply the service name filter to inbound packets, navigate to the service name filter prompt (for example, **box; ethernet 2/1; ipx 0x00023456; server-name-filter 00023456/myname**) and enter:

inbound disabled

By default, the router applies service name filters to outbound packets.If you do not want to apply the service name filter to outbound packets, navigate to the service name filter prompt (for example, **box; ethernet 2/1; ipx 0x00023456; server-name-filter 00023456/myname**) and enter:

outbound disabled

To apply the service name filter to outbound packets, navigate to the service name filter prompt (for example, **box; ethernet 2/1; ipx 0x00023456; server-name-filter 00023456/myname**) and enter:

outbound enabled

Using Site Manager

To apply the service name filter to inbound or outbound packets, or both, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Name Filter.**	The IPX Service Name Filters window opens.
5. Set the **Mode** parameter. Click on **Help** or see the parameter description on page B-86.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Protocol

When you send SAP updates, you can apply this outbound filter only to services learned on the specified protocol. This feature does not apply to inbound services.

By default, the outbound filter applies to any protocol. You can accept the default, any protocol, or specify that it apply to local, static, or SAP protocols.

Using the BCC

To apply an outbound filter to services learned on a specified protocol, navigate to the service name filter prompt (for example, **box; ethernet 2/1; ipx 0x00023456; server-name-filter 00023456/myname**) and enter:

protocol *protocol*

protocol is one of the following:

any
local
nlsp
static
sap

For example, to set the outbound filter to services learned on the SAP protocol, enter:

```
server-name-filter/00023456/myname# protocol sap
```

Using Site Manager

To apply an outbound filter to services learned on a specified protocol, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Global Parameters window opens.
4. Choose **Name Filter.**	The IPX Service Name Filters window opens.
5. Set the **Protocol** parameter. Click on **Help** or see the parameter description on page B-86.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying How to Process SAP Advertisements

You can specify how the router should process any SAP advertisement that matches the SAP filter criteria you established in the Target Service Name and Target Service Type parameters.

By default, the filter allows advertisement or acceptance of services that match the filter criteria you established in the Service Name and Service Type parameters.

You can accept the default or set the filter to cause the IPX router to suppress, or drop, SAP advertisements that match the SAP filter criteria you established.

Using the BCC

To specify how the router should process SAP advertisements, navigate to the service name filter prompt (for example, **box; ethernet 2/1; ipx 0x00023456; server-name-filter 00023456/myname**) and enter:

action *value*

value is one of the following:

Action	Meaning
Advertise	Enables the filter to allow advertisement or acceptance of routes that match the specified route filter criteria
Suppress	Causes the IPX router to drop advertisements that match the specified route filter criteria

For example, to enable the filter to accept routes that match the filter's criteria, enter:

```
server-name-filter/00023456/myname# action suppress
```

Using Site Manager

To specify how the router should process SAP advertisements, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Name Filter.**	The IPX Service Name Filters window opens.
5. Set the **Action** parameter. Click on **Help** or see the parameter description on page B-87.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying a Cost

If you are enabling the filter to allow advertisement or acceptance of services that match the filter criteria you established when you specified a service name and a service type, you can assign a cost (number of ticks or hops) for this interface.

The cost is included in subsequent SAP packets sent to other interfaces. IPX disposes of the packet when its hop count passes a value that is one less than the value of the maximum number of hops. This value must be the same across the network.

If the filter is an *inbound* filter, the entered cost replaces the cost associated with the server in the SAP advertisement, and the router uses this cost in its calculations.

If this is an *outbound* filter, the entered cost replaces the server's cost that is advertised in SAP packets by this router.

By default, the cost is set to 1. A zero cost indicates that the route's actual cost should be used.

Note: Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

Using the BCC

To assign a cost for a static service filter, navigate to the IPX static service prompt (for example, **box; ethernet 2/1; ipx 00023456; static-service/00023456/printer/0987**) and enter:

cost *integer*

integer is 1 to one less than the number of maximum hops for hop-based routing, or 1 to the maximum positive integer for tick-based routing.

For example, to set the cost to 120, enter:

```
static-service/00023456/printer/0987# cost 120
```

Using Site Manager

To assign a cost for a static service filter, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Static/Filter Tables**.	The IPX Static Interface Tables Configuration window opens.
4. Choose **Name Filter.**	The IPX Service Name Filters window opens.
5. Set the **Cost** parameter. Click on **Help** or see the parameter description on page B-88.	
6. Click on **OK**.	You return to the Configuration Manager window.

Deleting IPX from the Router

You can use the BCC or Site Manger to delete IPX from the router.

Using the BCC

To delete IPX from an interface, navigate to the IPX interface prompt (for example, **box; ipx**) and enter:

delete

To delete IPX globally from the router, navigate to the global IPX prompt (for example, **box; ipx**) and enter:

delete

Using Site Manager

To delete IPX from the router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPX**.	The IPX menu opens.
3. Choose **Delete IPX**.	A confirmation window opens.
4. Click on **OK**.	You return to the Configuration Manager window.

Note: If you delete IPX, the connectors for those interfaces on which IPX was the only protocol enabled are no longer highlighted in the Configuration Manager window. Interfaces must be reconfigured for these connectors; see *Configuring and Managing Routers with Site Manager* for instructions.

Appendix A
BCC IPX Parameters

This appendix explains all the IPX parameters available using the BCC and how to use them if you want to customize an interface you have added to a router.

Topic	Page
IPX Global Parameters	A-2
IPXWAN Parameters	A-6
Static NetBIOS Route Parameters	A-9
IPX Interface Parameters	A-10
IPX Adjacent Host Parameters	A-13
RIP Parameters	A-14
Route Filter Parameters	A-16
SAP Parameters	A-18
Server Name Filter Parameters	A-21
Server Network Filter Parameters	A-23
Static Route Parameters	A-25
Static Service Parameters	A-26

IPX Global Parameters

The IPX global parameters determine the way IPX works on the router. To configure IPX global parameters, navigate to the global IPX prompt (for example, **box; ipx**).

Table A-1. IPX Global Parameters

aging-frequency		
	Description:	Specifies how frequently, in seconds, that IPX checks to see whether any routes have timed out.
	Legal values:	<unsigned integer>
	Default value:	10
default-route		
	Description:	Enables or disables the router to use the default route, 0xFFFFFFFE, for IPX routing.
	Legal values:	enabled, disabled
	Default value:	enabled
destination-count		
	Description:	Specifies the maximum number of destinations (networks) that you expect the router to learn.
	Legal values:	<unsigned integer>
	Default value:	0
gns-response		
	Description:	Determines which server to choose when responding to a get_nearest_server request.
	Legal values:	alphabetical, last-learned
	Default value:	alphabetical
hops		
	Description:	Specifies the maximum number of hops an IPX packet may take to reach its destination.
	Legal values:	<unsigned integer>
	Default value:	16

(continued)

Table A-1. IPX Global Parameters *(continued)*

host-address		
	Description:	Specifies the value the router uses as a host address for all IPX interfaces. If left empty, the router uses the backplane serial number as the host address for all interfaces (circuits).
	Legal values:	<octet string: length 6 fill left>
	Default value:	<not_set>
host-count		
	Description:	Indicates the maximum next-hop hosts that you expect the router to learn
	Legal values:	<unsigned integer>
	Default value:	0
log-filter		
	Description	Specifies the type of log message that the router should filter.
	Legal values	debug, info,trace, debug-info, debug-trace, info-trace, debug-info-trace
	Default value	trace
maximum-path		
	Description	Specifies the maximum number of paths allowed for a given network destination and routing method.
	Legal values	<unsigned integer>
	Default value	1
mib-reply-slot		
	Description	Specifies the slot where the router sends MIB replies.
	Legal values	<string>
	Default value	{ }
multiple-host		
	Description	Enables or disables multiple host addressing.
	Legal values	enabled, disabled
	Default value	enabled

(continued)

Table A-1. IPX Global Parameters *(continued)*

network-table-size		
	Description	Specifies the size of the network table.
	Legal values	<unsigned integer>
	Default value	0
novell-certification-conformance		
	Description	Indicates whether you want the router to conform to Novell NetWare standards by propagating a NetBIOS Type 20 packet out of all its interfaces.
	Legal values	enabled, disabled
	Default value	enabled
path-splits		
	Description	Enables or disables IPX to do load balancing.
	Legal values	<unsigned integer>
	Default value	1
pend-frequency		
	Description:	Specifies the number of routes and services to age (process) before pending.
	Legal values:	<unsigned integer>
	Default value:	100
routing-method		
	Description:	Specifies for all slots the method of making IPX best-route decisions by either tick or hop based routing.
	Legal values:	hop, tick
	Default value:	tick
sap-via-default-route		
	Description:	Indicates whether a SAP advertisement can be learned from an interface if the network number advertised in the SAP advertisement is unreachable, but a default route is accessible from that interface.
	Legal values:	enabled, disabled
	Default value:	disabled

(continued)

Table A-1. IPX Global Parameters *(continued)*

service-count		
	Description:	Indicates the maximum number of services that you expect the router to learn.
	Legal values:	<unsigned integer>
	Default value:	0
state		
	Description:	Enables or disables the system software mechanisms that allow users to add IPX interfaces to the router configuration.
	Legal values:	enabled, disabled
	Default value:	enabled
table-fill-notify		
	Description:	Specifies the value the IPX router uses to notify you when the IPX network tale is filled.
	Legal values:	<unsigned integer>
	Default value:	100

IPXWAN Parameters

The IPXWAN parameters determine the way IPXWAN services operate on the router. To configure IPXWAN parameters, navigate to the global IPXWAN prompt (for example, **box; serial 3/1; ppp; ipxwan 00055555**).

Table A-2. IPXWAN Parameters

address		
	Description:	Specifies the address for this IPX interface.
	Legal values:	<octet string: length 4 fill left>
	Default value:	none
broadcast-address		
	Description:	Specifies a broadcast address for this IPX interface.
	Legal values:	<octet string>
	Default value:	0x
circuit-name		
	Description:	Specifies a symbolic name for the interface.
	Legal values:	<string>
	Default value:	{ }
cost		
	Description:	Sets the cost (number of ticks or hops) for this interface.
	Legal values:	<unsigned integer>
	Default value:	0
delay		
	Description:	Specifies the length of time, in microseconds, required to transmit 1 byte of data (excluding protocol headers) to a destination on the other end of this IPX circuit if the circuit is free of other traffic.
	Legal values:	<unsigned integer>
	Default value:	0
encapsulation		
	Description:	Specifies the encapsulation method for each circuit type.
	Legal values:	ethernet, lsap, novell, snap
	Default value:	lsap

(continued)

Table A-2. IPXWAN Parameters *(continued)*

host-address		
	Description	Specifies a host number that is unique within the IPX internetwork to this IPX interface.
	Legal values	<octet string>
	Default value	0x
multicast-address		
	Description	Specifies a multicast address for this IPX interface.
	Legal values	<octet string>
	Default value	0x
negotiated-protocol		
	Description	Indicates the protocol negotiated for this interface.
	Legal values	wan-rip, unnumbered-rip, wan-unnumbered-rips
	Default value	none
netbios-accept		
	Description	Enables or disables acceptance of all NetBIOS Type 20 (broadcast) packets received by this interface from an external source.
	Legal values	enabled, disabled
	Default value	disabled
netbios-deliver		
	Description	Enables or disables outbound delivery of all NetBIOS Type 20 (broadcast) packets received by this interface from another interface.
	Legal values	enabled, disabled
	Default value	disabled
primary-network		
	Description	Specifies an IPX network number for IPXWAN (RFC1634-compliant) link negotiation on all slots.
	Legal values	<octet string: length 4 fill left>
	Default value	none

(continued)

Table A-2. IPXWAN Parameters *(continued)*

router-name		
	Description	Specifies the symbolic name of the router.
	Legal values	<string (2...47)>
	Default value	none
stabilization-timer		
	Description	Determines the amount of traffic, in seconds, that RIP/SAP waits before sending out initial route information when a dial-on-demand route first becomes enabled.
	Legal values	<unsigned integer>
	Default value	0
state		
	Description:	Enables or disables IPX routing on this interface.
	Legal values:	enabled, disabled
	Default value:	enabled
svcbroadcast		
	Description:	Determines whether the router should establish frame relay SVCs for all adjacent hosts before sending RIP and SAP updates.
	Legal values:	enabled, disabled
	Default value:	disabled
throughput		
	Description:	Specifies the amount of time, in bits per second, that flow through an IPX circuit that is free of other traffic.
	Legal values:	<unsigned integer>
	Default value:	0
watchdog-spoofing		
	Description:	Specifies whether a router can respond locally to broadcast IPX watchdog packets on behalf of clients that use dial-in connections.
	Legal values:	enabled, disabled
	Default value:	disabled

Static NetBIOS Route Parameters

IPX static NetBIOS route parameters establish a NetBIOS static route To configure a static NEtBIOS route, .navigate to the static NetBIOS route prompt (for example, **box; ipx; static-netbios-route route6/00042567**).

Table A-3. Static NetBIOS Route Parameters

name		
	Description:	Specifies the name of a NetBIOS target server, which consists of a string of up to 16 alphanumeric characters (which can include wildcards and pattern-matching characters).
	Legal values:	<string (1...16)>
	Default value:	none
network		
	Description:	Specifies the address of a destination network that you want to recieve NetBIOS broadc ast packets destined for the specified target server.
	Legal values:	<octet string: length 4 fill left>
	Default value:	none
state		
	Description:	Enables or disables the static route record in the NetBIOS routing table.
	Legal values:	enabled, disabled
	Default value:	enabled

IPX Interface Parameters

IPX interface parameters determine how IPX behaves on individual router interfaces. To configure an individual IPX interface, navigate to the IPX interface prompt (for example, **box; ethernet 2/1; ipx 00023456**).

Table A-4. IPX Interface Parameters

address		
	Description:	Specifies the address for this IPX interface.
	Legal values:	<octet string: length 4 fill left>
	Default value:	none
broadcast-address		
	Description:	Specifies a broadcast address for this IPX interface.
	Legal values:	<octet string>
	Default value:	0x
circuit-name		
	Description:	Specifies a symbolic name for the interface.
	Legal values:	<string>
	Default value:	{ }
cost		
	Description:	Sets the cost (number of ticks or hops) for this interface.
	Legal values:	<unsigned integer>
	Default value:	0
delay		
	Description:	Specifies the length of time, in microseconds, required to transmit 1 byte of data (excluding protocol headers) to a destination on the other end of this IPX circuit if the circuit is free of other traffic.
	Legal values:	<unsigned integer>
	Default value:	0

(continued)

Table A-4. IPX Interface Parameters *(continued)*

encapsulation		
	Description:	Specifies the encapsulation method available for each circuit type.
	Legal values:	ethernet, lsap, novell, snap
	Default value:	lsap
end-station		
	Description:	Enables or disables source routing on this interface on a token ring circuit.
	Legal values:	enabled, disabled
	Default value:	disabled
host-address		
	Description	Specifies a host number that is unique within the IPX internetwork to this IPX interface.
	Legal values	<octet string>
	Default value	0x
multicast-address		
	Description	Specifies a multicast address for this IPX interface.
	Legal values	<octet string>
	Default value	0x
netbios-accept		
	Description	Enables or disables acceptance of all NetBIOS Type 20 (broadcast) packets received by this interface from an external source.
	Legal values	enabled, disabled
	Default value	disabled
netbios-deliver		
	Description	Enables or disables outbound delivery of all NetBIOS Type 20 (broadcast) packets received by this interface from another interface.
	Legal values	enabled, disabled
	Default value	disabled

(continued)

Table A-4. IPX Interface Parameters *(continued)*

stabilization-timer		
	Description	Determines the amount of time, in seconds, that RIP/SAP waits before sending out initial route information when a dial-on-demand route first becomes enabled.
	Legal values	<unsigned integer>
	Default value	0
state		
	Description:	Enables or disables IPX routing on this interface.
	Legal values:	enabled, disabled
	Default value:	enabled
svcbroadcast		
	Description:	Determines whether the router should establish frame relay SVCs for all adjacent hosts before sending RIP and SAP updates.
	Legal values:	enabled, disabled
	Default value:	disabled
throughput		
	Description:	Specifies the amount of traffic, in bits per second, that can flow through an IPX circuit if the circuit is free of other traffic.
	Legal values:	<unsigned integer>
	Default value:	0

IPX Adjacent Host Parameters

IPX adjacent hosts parameters establish an adjacent host. To configure IPX adjacent host parameters, navigate to the adjacent host prompt (for example, **box; ethernet 2/1; ipx 00023456; adjacent-host host-address 000012345678**).

Table A-5. IPX Adjacent Host Parameters

host-address		
	Description:	Specifies the address, in hexadecimal notation, of the IPX adjacent host.
	Legal values:	<octet string: length 6 fill left>
	Default value:	none
state		
	Description:	Enables or disables the IPX adjacent host.
	Legal values:	enabled, disabled
	Default value:	enabled
subaddress		
	Description:	Specifies the address of the remote host when establishing a SVC to the adjacent host.
	Legal values:	<string>
	Default value:	{ }
type		
	Description:	Specifies the type of static host used to establish an SVC connection to the adjacent host.
	Legal values:	default
	Default value:	default
type-of-number		
	Description:	Specifies the type of number, international or unknown, used when creating an SVC to an adjacent host.
	Legal values:	unknown, international
	Default value:	international

(continued)

Table A-5. IPX Adjacent Host Parameters *(continued)*

wan-number		
	Description:	Specifies a WAN address of up to 16 hexadecimal characters on an ATM or SMDS network, or a DLCI number on a frame relay network.
	Legal values:	<string (1...15)>
	Default value:	<not_set>

RIP Parameters

IPX RIP circuit parameters determine the way RIP behaves on a particular circuit.To configure RIP parameters, navigate to the RIP prompt (for example, **box; ethernet 2/1; ipx 00023456; rip 00023456**).

Table A-6. RIP Parameters

age-multiplier		
	Description:	Specifies the holding multiplier as the number of update intervals for information received in RIP periodic updates.
	Legal values:	<unsigned integer>
	Default value:	3
default-listen		
	Description:	Specifies if the router accepts the default route, 0xFFFFFFE, in RIP packets received on this circuit.
	Legal values:	enabled, disabled
	Default value:	disabled
default-supply		
	Description:	Enables or disables the router to advertise a default route, 0xFFFFFFE, if it exists in the routing table.
	Legal values:	enabled, disabled
	Default value:	disabled

(continued)

Table A-6. RIP Parameters *(continued)*

listen		
	Description:	Specifies that this interface listens to RIP periodic and triggered updates from neighboring networks and conveys received routing information to its internal routing table.
	Legal values:	enabled, disabled
	Default value:	enabled
multicast		
	Description:	Enables or disables the use of a multicast address to send RIP packets.
	Legal values:	enabled, disabled
	Default value:	enabled
pace		
	Description:	Specifies the maximum pace (in packets per second) at which RIP packets can be sent on this circuit.
	Legal values:	<unsigned integer>
	Default value:	18
packet-size		
	Description:	Specifies the maximum RIP packet size, in bytes, used on this circuit.
	Legal values:	<unsigned integer>
	Default value:	432
split-horizon		
	Description:	Enables or disables the interface to exclude RIP routes learned on that interface when transmitting RIP updates.
	Legal values:	enabled, disabled
	Default value:	enabled
state		
	Description:	Enables or disables RIP on this interface.
	Legal values:	enabled, disabled
	Default value:	enabled

(continued)

Table A-6. RIP Parameters *(continued)*

supply		
	Description:	Specifies that the interface transmits all RIP periodic and triggered updates to routers in neighboring networks.
	Legal values:	enabled, disabled
	Default value:	enabled
triggered-update		
	Description:	Enables or disables the router to immediately propagate change in status information to other routers in the internetwork.
	Legal values:	enabled, disabled
	Default value:	enabled
update-interval		
	Description:	Adjusts the frequency of RIP update packet transmissions, in seconds, for this circuit.
	Legal values:	<unsigned integer>
	Default value:	60

Route Filter Parameters

Router filters enable or disable inbound or outbound traffic from specified protocols. To configure route filter parameters, navigate to the route filter prompt (for example, **box; ipx 00023456; route-filter 0x8888/0x2121**).

Table A-7. Route Filter Parameters

action		
	Description:	Specifies how to process any RIP advertisement that matches the route filter criteria you established.
	Legal values:	advertise, suppress
	Default value:	advertise

(continued)

Table A-7. Route Filter Parameters *(continued)*

cost		
	Description:	Assigns a cost, in ticks or hops, for routes matching this filter.
	Legal values:	<unsigned integer>
	Default value:	0
inbound		
	Description:	Applies the filter to RIP packets coming into this interface.
	Legal values:	enabled, disabled
	Default value:	disabled
mask		
	Description:	Specifies an 8-digit hexadecimal mask that you want to apply
	Legal values:	<octet string: length 4 fill left>
	Default value:	none
network		
	Description:	Identifies the network on which you want to apply the filter.
	Legal values:	<octet string: length 4 fill left>
	Default value:	none
outbound		
	Description:	Applies the filter to RIP packets going out of this interface.
	Legal values:	enabled, disabled
	Default value:	disabled
priority		
	Description:	Specifies the priority of this filter in relation to other filters of the same type.
	Legal values:	<unsigned integer>
	Default value:	0

(continued)

Table A-7. Route Filter Parameters *(continued)*

protocol		
	Description:	Applies this filter only to routes learned on the specified protocol when sending RIP updates.
	Legal values:	any, local, rip, nlsp, static
	Default value:	any
state		
	Description:	Enables or disables a route filter previously added to a specific IPX interface.
	Legal values:	enabled, disabled
	Default value:	enabled

SAP Parameters

IPX SAP circuit parameters determine the way SAP behaves on a particular circuit.To configure SAP parameters, navigate to the SAP prompt (for example, **box; ethernet 2/1; ipx 00023456; sap 00023456**)

Table A-8. SAP Parameters

age-multiplier		
	Description:	Specifies the holding multiplier as the number of update intervals for information received in RIP periodic updates.
	Legal values:	<unsigned integer>
	Default value:	3
listen		
	Description:	Specifies that this interface listens to SAP periodic and triggered updates from neighboring networks and conveys received routing information to its internal routing table.
	Legal values:	enabled, disabled
	Default value:	enabled

(continued)

Table A-8. SAP Parameters *(continued)*

multicast		
	Description:	Enables or disables the use of a multicast address to send SAP packets.
	Legal values:	enabled, disabled
	Default value:	enabled
nearest-server-reply		
	Description:	Enables or disables the the router to respond to get_nearest_server requests.
	Legal values:	enabled, disabled
	Default value:	enabled
nsq-alphabetical		
	Description:	Enables or disables the router to respond to a get_nearest_server request alphabetically.
	Legal values:	enabled, disabled
	Default value:	enabled
pace		
	Description:	Specifies the number of SAP maximum packets per second that the router can send SAP on this circuit.
	Legal values:	<unsigned integer>
	Default value:	18
packet-size		
	Description:	Specifies the maximum SAP packet size, in bytes, used on this circuit.
	Legal values:	<unsigned integer>
	Default value:	480
save-full-name		
	Description:	Enables or disables the router to either save all 48 bytes in the service name field of SAP packets or ignore all characters after the null character when a service field name is less than 48 bytes.
	Legal values:	enabled, disabled
	Default value:	enabled

(continued)

Table A-8. SAP Parameters *(continued)*

split-horizon		
	Description:	Determines if the interface includes SAP routes learned on the interface when transmitting SAP updates.
	Legal values:	enabled, disabled
	Default value:	enabled
state		
	Description:	Enables or disables SAP on this interface.
	Legal values:	enabled, disabled
	Default value:	enabled
supply		
	Description:	Determines if the interface transmits all SAP periodic and triggered updates to routers in neighboring networks.
	Legal values:	enabled, disabled
	Default value:	enabled
triggered-update		
	Description:	Enables or disables the router to immediately propagate change in status information to other routers in the internetwork.
	Legal values:	enabled, disabled
	Default value:	enabled
update-interval		
	Description:	Adjusts the frequency of SAP update packet transmissions, in seconds, for this circuit.
	Legal values:	<unsigned integer>
	Default value:	60

Server Name Filter Parameters

The server name filters function lets you reduce network traffic by configuring server name filters. To configure server name filter parameters, navigate to the server name filter prompt (for example, **box; ethernet 2/1; ipx 0x00023456; server-name-filter 00023456/myname**)

Table A-9. Server Name Filter Parameters

action		
	Description:	Specifies how to process RIP advertisements that match the server name filter criteria.
	Legal values:	advertise, suppress
	Default value:	advertise
cost		
	Description:	Assigns a cost, in ticks or hops, for routes matching this filter.
	Legal values:	<unsigned integer>
	Default value:	0
inbound		
	Description:	Applies the filter to RIP packets coming into this interface.
	Legal values:	enabled, disabled
	Default value:	disabled
name		
	Description:	Specifies the server name.
	Legal values:	<string (2...47)>
	Default value:	none
outbound		
	Description:	Applies the filter to RIP packets going out of this interface.
	Legal values:	<string (2...47)>
	Default value:	none

(continued)

Table A-9. Server Name Filter Parameters *(continued)*

priority		
	Description:	Specifies the priority of this filter in relation to other filters of the same type.
	Legal values:	<unsigned integer>
	Default value:	0
protocol		
	Description:	Applies this filter to routes learned on the specified protocol when sending RIP updates.
	Legal values:	any, local, nlsp, static, sap
	Default value:	any
state		
	Description:	Enables or disables a server name filter previously added to a specific IPX interface.
	Legal values:	enabled, disabled
	Default value:	enabled
type		
	Description:	Specifies the type of server, using 4-digit hexadecimal Novell server types.
	Legal values:	<octet string>
	Default value:	0x

Server Network Filter Parameters

Service network filter parameters determine which SAP broadcasts to pass to the locally attached network segment. To configure server network filter parameters, navigate to the server network filter prompt (for example, **box; ethernet 2/1; ipx 0x00023456; server-network-filter/00000999/00000888/00000065**).

Table A-10. Server Network Filter Parameters

action		
	Description:	Specifies how to process any RIP advertisement that matches the route filter criteria you established..
	Legal values:	advertise, suppress
	Default value:	advertise
cost		
	Description:	Assigns a cost, in ticks or hops, for routes matching this filter.
	Legal values:	<unsigned integer>
	Default value:	0
inbound		
	Description:	Applies the filter to RIP packets coming into this interface.
	Legal values:	enabled, disabled
	Default value:	disabled
mask		
	Description:	Specifies a valid IPX network address in hexadecimal notation that determines which networks will be filtered.
	Legal values:	<octet string: length 4 fill left>
	Default value:	none
network		
	Description:	Specifies the network on which you want to apply the service network filter.
	Legal values:	<octet string: length 4 fill left>
	Default value:	none

(continued)

Table A-10. Server Network Filter Parameters *(continued)*

outbound		
	Description:	Applies this filter to RIP packets going out of this interface.
	Legal values:	enabled, disabled
	Default value:	enabled
priority		
	Description:	Specifies the priority of this filter in relation to other filters of the same type.
	Legal values:	<unsigned integer>
	Default value:	0
protocol		
	Description:	Applies this filter to routes learned on the specified protocol when sending RIP updates.
	Legal values:	any, local, nlsp, static, sap
	Default value:	any
state		
	Description:	Enables or disables a server network filter displayed on this interface.
	Legal values:	enabled, disabled
	Default value:	enabled
type		
	Description:	Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.
	Legal values:	<octet string>
	Default value:	0x

Static Route Parameters

IPX static route parameters establish a static route. To configure IPX static route parameters, navigate to the static route prompt (for example, **box; ethernet/2/1; ipx 00023456; static-route 00023456/00054321/000000765432**).

Table A-11. Static Route Parameters

hops		
	Description:	Specifies the number of hops required for an IPX datagram to traverse this static route.
	Legal values:	<unsigned integer >
	Default value:	0
next-hop-host		
	Description:	Specifies the host address, in up to 12 hexadecimal characters, of the down-stream router's IPX interface.
	Legal values:	<octet string: length 6 fill left>
	Default value:	none
state		
	Description:	Enables or disables the static route record in the IPX routing tables.
	Legal values:	enabled, disabled
	Default value:	enabled
target-network		
	Description:	Specifies the address of the network to which you want to configure the static route.
	Legal values:	<octet string: length 4 fill left>
	Default value:	none
ticks		
	Description:	Specifies the number of 1/18th-second timer ticks required for an IPX datagram to traverse this static route.
	Legal values:	<unsigned integer>
	Default value:	0

Static Service Parameters

IPX static service parameters establish a static NetWare service for each interface on a Bay Networks router. To configure IPX static service parameters, navigate to the IPX static service prompt (for example, **box; ethernet 2/1; ipx 00023456; static-service/00023456/printer/0987**).

Table A-12. Static Service Parameters

hops		
	Description:	Specifies the number of subsequent router hops required from this router to reach a specific remote Novell server or service.
	Legal values:	<unsigned integer>
	Default value:	1
host-address		
	Description:	Specifies the address of a remote IPX host (a NetWare server) that can provide local clients with specific NetWare services, such as file, print, gateway, or terminal server services.
	Legal values:	<octet string>
	Default value:	0x
name		
	Description:	Assigns a symbolic name to the service you want to advertise.
	Legal values:	<string (2...47)>
	Default value:	none
network		
	Description:	Specifies the network address, in hexadecimal notation, of this service.
	Legal values:	<octet string>
	Default value:	none

(continued)

Table A-12. Static Service Parameters *(continued)*

socket		
	Description:	Specifies the socket address of this service.
	Legal values:	<octet string>
	Default value:	0
state		
	Description:	Enables or disables a static service previously added to a specific IPX interface.
	Legal values:	enabled, disabled
	Default value:	enabled
type		
	Description:	Specifies the type of service to advertise from the associated IPX (LAN) interface.
	Legal values:	<octet string: length 2 fill left>
	Default value:	none

Appendix B
Site Manager IPX Parameters

This appendix explains all IPX parameters and how to use them to create and customize an IPX interface.

Topic	Page
IPX Configuration Parameters	B-2
IPXWAN Configuration Parameters	B-7
IPX Global Parameters	B-9
IPX Advanced Global Parameters	B-13
IPX Interface Parameters	B-22
IPX Change Circuit Parameters	B-30
IPX RIP Circuit Parameters	B-35
IPX SAP Circuit Parameters	B-41
IPX NetBIOS Static Route Configuration Parameters	B-46
IPX NetBIOS Static Route Parameters	B-48
Adjacent Host Configuration Parameters	B-50
IPX Adjacent Hosts Parameters	B-53
IPX Static Route Configuration Parameters	B-56
IPX Static Route Parameter Descriptions	B-59
IPX Static Service Configuration Parameters	B-61
IPX Static Service Parameters	B-64
Route Filter Configuration Parameters	B-67
IPX Route Filter Parameters	B-74
Service Network Filter Configuration Parameters	B-74
IPX Service Network Filter Parameters	B-77

Topic	Page
IPX Service Name Filter Configuration Parameters	B-82
IPX Service Name Filter Parameters	B-84

IPX Configuration Parameters

The IPX configuration parameters enable you to get IPX up and running quickly by supplying only the required configuration information and accepting the defaults supplied by Bay Networks for all other Site Manager parameters. You access these parameters from the IPX Configuration window (Figure B-1). This window may look different depending on the WAN protocol you chose in the Select WAN Protocols window.

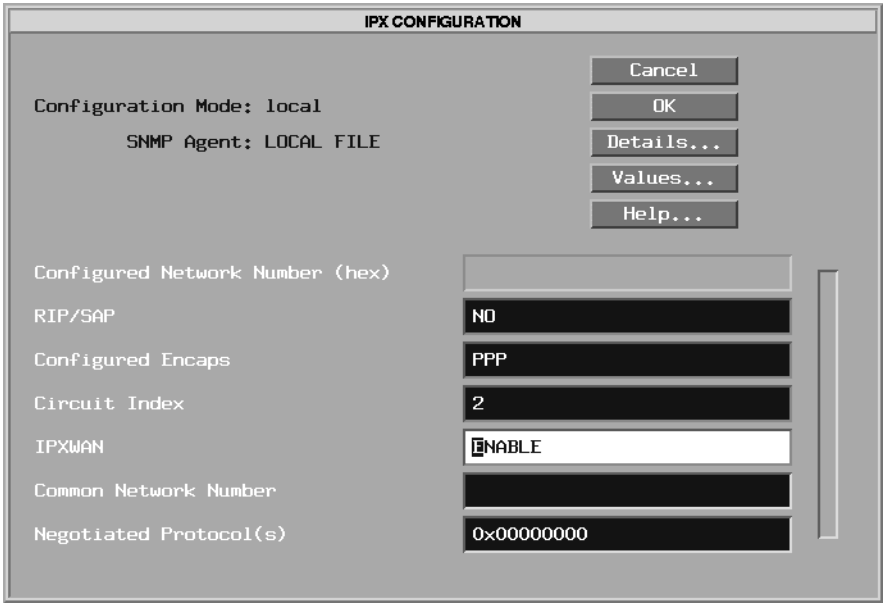

Figure B-1. IPX Configuration Window

Note: The Configured Network Number parameter is active only for circuits that are not configured as IPXWAN interfaces. The IPXWAN, Common Network Number, and Negotiated Protocol(s) parameters appear only when the circuit is configured as an IPXWAN interface.

Parameter: Configured Network Number (hex)

Path: Configuration Manager > Select Protocols > IPX > Interfaces

Default: None

Options: Any valid IPX network number in hexadecimal format

Function: Identifies the IPX network number assigned to this IPX circuit. This parameter is active only for circuits that are not configured as IPXWAN interfaces or for those with the IPXWAN parameter explicitly disabled.

Instructions: Enter a valid IPX network number in hexadecimal notation.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.22

Parameter: RIP/SAP

Path: Configuration Manager > Select Protocols > IPX > Interfaces

Default: Depends on whether you enabled RIP/SAP in the Select Protocols window

Options: Yes | No

Function: Indicates whether you have RIP/SAP configured on an interface.

Instructions: The Configuration Manager sets the default for this parameter based on your selection in the Select Protocols window. If you selected RIP/SAP, both RIP and SAP are enabled. You can disable both RIP and SAP using the IPX Configuration window. You can also disable and reenable RIP or SAP using the RIP Circuit window or the SAP Circuit window, which are accessible from the IPX Interfaces window.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.1 (RIP)

1.3.6.1.4.1.18.3.5.5.33.1.1 (SAP)

Parameter: Configured Encaps

Path: Configuration Manager > Select Protocols > IPX > Interfaces

Default: Circuit media dependent

Options: Ethernet | LSAP | Novell | SNAP | PPP

Function: Specifies the encapsulation method (such as Ethernet, PPP, Novell, LSAP, or SNAP) available for each circuit type (such as Ethernet, token ring, or serial). The encapsulation method supports communication on a specific logical network.

Instructions: Select an encapsulation method that matches the one that the clients and servers on the same logical network use and is appropriate for the physical circuit, as follows:

- Ethernet circuits support Ethernet, LSAP, Novell, and SNAP frames.
- Token ring circuits support LSAP and SNAP frames.
- Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21, T1/E1) support SNAP, PPP, and X.25 Point-to-Point (Ethernet) frames.
- FDDI circuits support LSAP and SNAP frames.
- HSSI circuits support PPP and SNAP frames.
- ISDN circuits support PPP frames.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.40

Parameter: Circuit Index

Path: Configuration Manager > Select Protocols > IPX > Interfaces
Default: System-assigned
Options: Any valid circuit identifier
Function: Uniquely identifies this circuit within this instance of IPX.
Instructions: Accept the default or enter a valid circuit identifier.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.6

Parameter: IPXWAN

Path: Configuration Manager > Select Protocols > IPX > Interfaces
Default: Enable
Options: Enable | Disable
Function: Enables or disables IPXWAN for this interface on the router. This parameter is active only for circuits that are configured as IPXWAN interfaces.
Instructions: Select Enable to turn on IPXWAN negotiation for this interface. Select Disable to turn off IPXWAN negotiation for this interface.
MIB Object ID: Not Applicable

Parameter: Common Network Number

Path: Configuration Manager > Select Protocols > IPX > Interfaces
Default: None
Options: Any valid IPX network number, 0x00000000 to 0xFFFFFFFD, in hexadecimal format
Function: Specifies the IPX common network number assigned to this IPX circuit. This parameter is active only for circuits that are configured as IPXWAN interfaces that have the IPXWAN parameter enabled.
Instructions: Enter a valid IPX network number in hexadecimal format. Do not use the values 0xFFFFFFFE or 0xFFFFFFFF as network numbers. These values are reserved for system use.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.24

Parameter:	**Negotiated Protocol(s)**
Path:	Configuration Manager > Select Protocols > IPX > Interfaces
Default:	Unnumbered RIP
Options:	RIP | Unnumbered RIP
Function:	Indicates the protocol negotiated for this interface. This parameter is active only for circuits that are configured as IPXWAN interfaces and that have the IPXWAN parameter enabled.
Instructions:	Accept the default or click on Values to display the other choices. You can select more than one option. Click on the options you prefer, then click on OK to accept your choices. The parameter value appears as a hexadecimal number in the IPX Change Circuit window. The values are as follows: 0x00000008 -- RIP 0x00000010 -- Unnumbered RIP 0x00000018 -- RIP and Unnumbered RIP
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.8

IPXWAN Configuration Parameters

The IPX configuration parameters enable you to get IPX using IPXWAN services up and running quickly by supplying only the required configuration information and accepting the defaults supplied by Bay Networks for all other Site Manager parameters. You access these parameters via the IPXWAN Configuration window (Figure B-2). This window opens after you enable IPXWAN services in the IPX Configuration window.

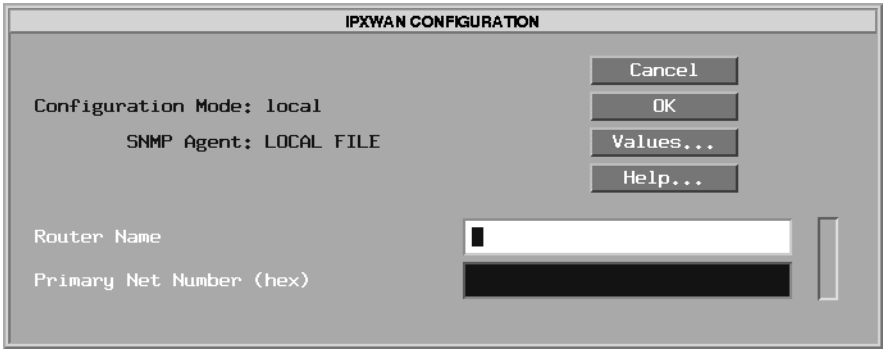

Figure B-2. IPXWAN Configuration Window

Parameter: Router Name

Path: Configuration Manager > Select Protocols > IPX > Enable IPXWAN

Default: None

Options: Any valid NetWare router or server name

Function: Specifies a symbolic name for the router. Any IPXWAN (RFC 1634-compliant) interface on the node uses this name to identify itself to the IPX router or server at the opposite end of the WAN data link.

The symbolic name for the router must be unique among those assigned to IPX file servers and routers anywhere in the IPX internetwork.

Instructions: See the documentation that came with your NetWare operating system for guidelines on specifying a router or server name. You should make the name meaningful to users.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.15.1.9

Parameter:	**Primary Net Number (hex)**
Path:	Configuration Manager > Select Protocols > IPX > Enable IPXWAN
Default:	None
Options:	A string of up to 8 hexadecimal characters
Function:	Specifies an IPX network number for IPXWAN (RFC 1634-compliant) link negotiation on all slots. The value of the primary network number (PNN) determines whether the local or remote WAN interface serves as IPX lLink master. The node with the highest PNN value becomes the IPX link master. The PNN must be unique among network numbers currently assigned.
Instructions:	Enter a unique network number for each node requiring one or more IPXWAN (RFC 1634-compliant) interfaces. (This network number must be unique across the IPX network. Do not enter a number that a server is using as an internal network number, or a number that has been assigned on any segment in the network.) You can use any unused value between 0x00000001 and 0xFFFFFFFD.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.15.1.5

IPX Global Parameters

The IPX global parameters determine the way IPX works on the router. You access these parameters in the Edit IPX Global Parameters window (Figure B-3).

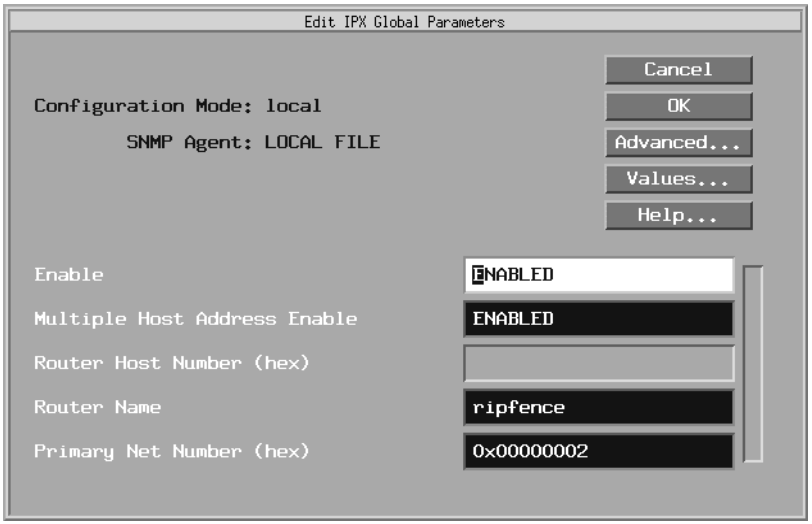

Figure B-3. Edit IPX Global Parameters Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Global

Default: Enable

Options: Enable | Disable

Function: Globally enables or disables the system software mechanisms that allow users to add IPX interfaces to the router configuration:

Disable -- Shuts down all IPX routing for the entire router.

Enable -- Initializes IPX routing for the entire router. Associated IPX interfaces become active, depending on their respective Enable parameters and on the state of each underlying circuit.

Instructions: Select Disable to disable every IPX interface on the router.

Select Enable to globally reinitialize all IPX interfaces on the router; each interface maintains the most recent setting of its own interface Enable parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.15.1.2

Parameter: Multiple Host Address Enable

Path: Configuration Manager > Protocols > IPX > Global

Default: Enable

Options: Enable | Disable

Function: If you enable this parameter, an IPX interface can:

- Use the MAC address located in the PROM on the circuit associated with that interface.
- Use a MAC address that you enter in the Host Number (hex) parameter field for that interface. Interfaces on a token ring circuit adopt a host ID number based only on the MAC address of the associated circuit.

Disabling this parameter causes all IPX interfaces to adopt a single host ID number for the entire host, based either on the serial number of the router backplane or on a number that you enter in the Host Number (hex) parameter field.

Instructions: Choose Enable or Disable, as appropriate for the type of configuration.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.15.1.6

Parameter: **Router Host Number (hex)**

Path: Configuration Manager > Protocols > IPX > Global

Default: None

Options: Any valid host number

Function: The router either uses this value as the host address for all IPX interfaces, or, if left empty, uses the backplane serial number as the host address for all interfaces (circuits).

Instructions: If you disable the Multiple Host Address Enable parameter and enter a unique router host number, the Configuration Manager assigns this number to all IPX interfaces you configure on the router.

If you disable the Multiple Host Address Enable parameter and do *not* enter a router host id number for this parameter, the Configuration Manager automatically generates a unique 6-byte host ID number for all IPX interfaces. The generated host ID is based on the serial number of the router backplane.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.15.1.7

Caution: The IPX global host address and the token ring MAC address must agree when the Multiple Host Address Enable parameter is disabled.

Parameter: **Router Name**

Path: Configuration Manager > Protocols > IPX > Global

Default: None

Options: Any valid NetWare router or server name

Function: Specifies a symbolic name for the router. Any IPXWAN (RFC 1634-compliant) interface on the node uses this name to identify itself to the IPX router or server at the opposite end of the WAN data link.

The symbolic name for the router must be unique among those assigned to IPX file servers and routers anywhere in the IPX internetwork.

Instructions: See the documentation that came with your NetWare operating system for guidelines on specifying a router or server name. You should make the name meaningful to users.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.15.1.9

Parameter:	**Primary Net Number (hex)**
Path:	Configuration Manager > Protocols > IPX > Global
Default:	None
Options:	A string of up to 8 hexadecimal characters
Function:	Specifies an IPX network number for IPXWAN (RFC 1634-compliant) link negotiation on all slots. The value of the primary network number (PNN) determines whether the local or remote WAN interface serves as IPX link master. The node with the higher PNN value becomes the IPX link master. The PNN must be unique among network numbers currently assigned.
Instructions:	Enter a unique network number for each node requiring one or more IPXWAN (RFC 1634-compliant) interfaces. (This network number must be unique across the IPX network. Do not enter a number that a server is using as an internal network number, or a number that has been assigned on any segment in the network.) You can use any unused value between 0x00000001 and 0xFFFFFFFD.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.15.1.5

IPX Advanced Global Parameters

IPX advanced global parameters enable you to fine-tune the way IPX runs on the router. You access these parameters in the Edit IPX Advanced Global Parameters window (Figure B-4). To view all of the parameters in this window, click on the scroll bar.

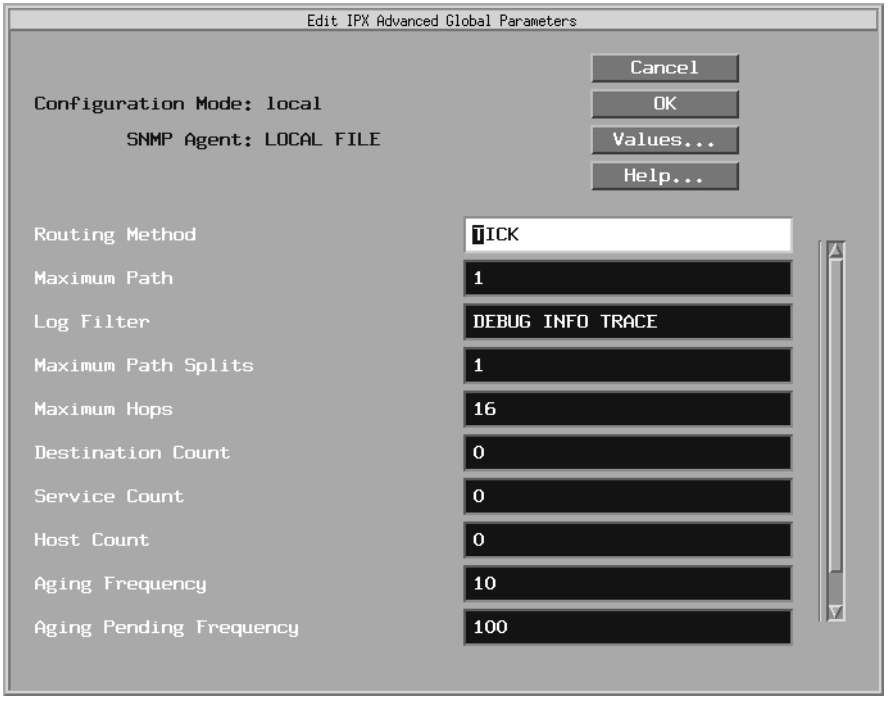

Figure B-4. IPX Advanced Global Parameters Window

Parameter: Routing Method

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: Tick

Options: Hop │ Tick

Function: Specifies for all slots the method of making IPX "best-route" decisions by:

Ticks -- The amount of time, expressed in ticks, that a packet requires to reach another network segment. (Each tick = 1/18th of a second.)

Hops -- The number of router hops a packet must traverse to reach another network segment.

If you accept the default, Tick, and the router knows about two paths to a network, and both paths have equal tick values, the router chooses the path with the smallest number of hops.

If you select Hop, and the best routes result in the same number of ticks, the router makes its decision based only on hops.

Instructions: Choose the method that results in the best routing performance. Usually, the best route is the one with:

- The lowest number of ticks for a packet to reach a node on the destination network
- The lowest number of hops (if multiple routes exist with equal numbers of ticks for a packet to reach a node on the destination network)

If routes exist with equal numbers of ticks and hops, choose either method. Bay Networks recommends using the default (tick-based) method, because tick-based routing takes into account actual link delay in determining the best path between IPX networks. Thus, it provides a more accurate routing mechanism than "hop count."

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.3

Parameter: Maximum Path

Path:	Configuration Manager > Protocols > IPX > Global > Advanced
Default:	1
Options:	1 to 1,023
Function:	Specifies the maximum number of paths allowed for a given network destination and routing method.
Instructions:	Set this parameter to the highest number of paths, from 1 to 1,023, that exist from the router to any destination network, regardless of cost.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.5

Parameter: Log Filter

Path:	Configuration Manager > Protocols > IPX > Global > Advanced
Default:	Trace
Options:	None | Debug | Info | Trace | Debug Info | Debug Trace | Info Trace | Debug Info Trace
Function:	Filters out the specified type of log message. For example, the default setting (Trace) filters out trace messages.
Instructions:	Do not change the default value of this parameter unless you are an experienced IPX user. Changing the value of this parameter produces significant global effects on memory allocation within the router, and these changes can significantly affect router performance. If you are an experienced user, enter a filtering mode that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.4

Parameter:	**Maximum Path Splits**
Path:	Configuration Manager > Protocols > IPX > Global > Advanced
Default:	Enable
Options:	Enable | Disable
Function:	If enabled, IPX will do load balancing to a particular destination up to the number of paths specified using the Maximum Path parameter.
Instructions:	Accept the default (Enable) to do load balancing on the number of equal cost paths specified in the Maximum Path parameter. If you disable this parameter, IPX uses only the lowest-cost path to send data to a destination network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.6

Parameter:	**Maximum Hops**
Path:	Configuration Manager > Protocols > IPX > Global > Advanced
Default:	16
Options:	1 to 255
Function:	Specifies the maximum number of hops an IPX packet can take to reach its destination.
Instructions:	Accept the default (16) or specify an integer from 1 to 255. In the case of RIP, every node in the network should use the same Maximum Hops parameter value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.7

Parameter: Destination Count

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: 0

Options: 0 to 5000

Function: Specifies the maximum number of destinations (networks) for the router to learn. IPX uses this value to preallocate table sizes for forwarding and network tables. If you specify 0, the default value, IPX dynamically allocates the amount of memory it needs for the tables. Changing this value can greatly affect the memory use by IPX, but it can also speed learning time for the router.

Instructions: Do not change the default value of this parameter unless you are an experienced IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value of this parameter can significantly affect router performance. If you are an experienced user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.17

Parameter: Service Count

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: 1

Options: 1 to 5000

Function: Indicates the maximum number of services for the router to learn. IPX uses this value to preallocate table sizes for service tables. If you specify 0, the default value, IPX automatically allocates the amount of memory it needs for the tables. Changing this value can greatly affect the memory used by IPX, but it can also speed learning time for the router.

Instructions: Do not change the default value of this parameter unless you are an experienced IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value of this parameter can significantly affect router performance. If you are an experienced user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.19

Parameter: Host Count

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: 1

Options: 1 to 5000

Function: Indicates the maximum number of next-hop hosts for the router to learn. IPX uses this value to preallocate table sizes for host tables. Changing this value can greatly affect the memory used by IPX, but it can also speed learning time for the router.

Instructions: Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.21

Parameter: Aging Frequency

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: 10

Options: 1 to the maximum positive integer (seconds)

Function: Specifies the interval, in seconds, for aging RIP and SAP information. IPX checks whether any routes have timed out every *n* seconds, where *n* is the interval that this parameter specifies.

Instructions: Do not change the default value of this parameter unless you are an experienced IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value of this parameter can significantly affect router performance. If you are an experienced user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.23

Parameter: **Aging Pending Frequency**

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: 100

Options: 1 to maximum number of routes and services

Function: Specifies the number of routes and services to age (process) before pending. A higher number lets the aging process proceed more quickly.

Instructions: Do not change the default value of this parameter unless you are an experienced IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value of this parameter can significantly affect router performance. If you are an experienced user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.24

Parameter: **Default Route**

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: Enable

Options: Enable | Disable

Function: Globally enables or disables the use of the default route 0xFFFFFFFE for IPX routing.

Enable -- Directs the router to use the default route (if one exists in its routing table) when it receives an IPX packet that does not contain a known IPX destination address within the IPX protocol header.

Disable -- Forces the router to drop a packet whose destination address is unknown, even if a default route exists.

Instructions: Select Enable to allow IPX default routing. Select Disable to turn off default routing.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.25

Parameter: **SAP via Default Route**

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: Disable

Options: Enable | Disable

Function: Indicates whether a SAP advertisement can be learned from an interface if the network number advertised in the SAP advertisement is unreachable, but a default route is accessible from that interface.

Enable -- Directs the router to accept a service when a direct or default route to the server is known.

Disable -- Accepts a service only when a direct route to the server advertising the service is known.

This feature gives you the option of making SAP entries available when the IPX default route is reachable.

Instructions: Select Enable to enable IPX default routing globally for SAP advertisements. Select Disable to turn off default SAP advertisement routing.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.26

Caution: Because this feature deviates from the IPX Default Route specification, enabling it may cause the interface to be incompatible with other router implementations.

Parameter: **Novell Certification Conformance**

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: Enable

Options: Enable | Disable

Function: Indicates whether you want the router to conform to Novell NetWare standards by propagating a NetBIOS type 20 packet out all its interfaces.

Instructions: Accept the default, Enable, if you want the router to propagate NetBIOS type 20 packets out all its interfaces (conforming to Novell standards). Select Disable if you configured NetBIOS static routes and you want the router to direct a packet to its destination network. You must set the same option (Enable or Disable) for all routers in the network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.15

Parameter: **GNS Response Mode**

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: Alphabetical

Options: Alphabetical | Last Learned

Function: Determines the server to choose when responding to a get_nearest_server (GNS)request.

Instructions: Accept the default to sort through all server names alphabetically. Select Last Learned to choose the last server learned.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.29

IPX Interface Parameters

IPX interface parameters determine how IPX behaves on individual router interfaces. You access these parameters in the IPX Interfaces window (Figure B-5). To view all parameters in this window, click on the scroll bar.

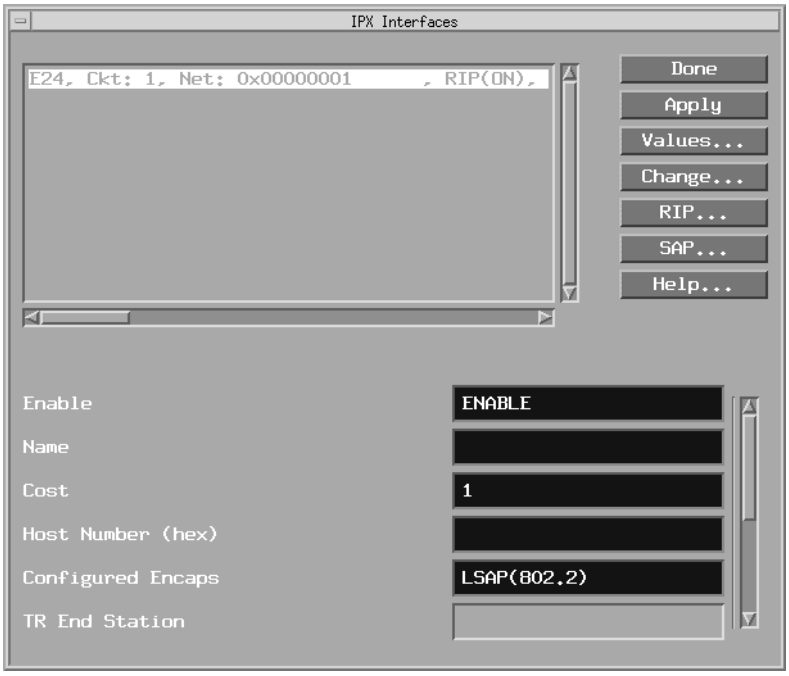

Figure B-5. IPX Interfaces Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: Enable

Options: Enable | Disable

Function: Enables or disables IPX routing on this interface.

Enable -- Initializes the IPX interface you added to a circuit. You can also use the Enable setting to reinitialize an existing disabled IPX interface. The actual operating state of an interface, when enabled, depends on:

- The current state of the associated circuit
- The current state of the IPX global protocol process

Disable -- Forces an IPX interface into the down (inoperative) state

Instructions: Select Enable if you previously set this parameter to Disable and now want to reenable IPX routing on this interface.

Select Disable only if you want to disable IPX routing on this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.2

Parameter: Name

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: None

Options: Any valid IPX server name

Function: Specifies a symbolic name for the interface.

Instructions: See the documentation that came with your NetWare operating system for guidelines on specifying a host, interface, router, or server name. You should make the name meaningful to users.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.7

Parameter:	**Cost**
Path:	Configuration Manager > Protocols > IPX > Interfaces
Default:	0
Options:	0 to the maximum positive integer (if tick-based routing is enabled) 0 to one less than the value specified using the advanced global Maximum Hops parameter (if hop-based routing is enabled)
Function:	Sets the cost (number of ticks or hops) for this interface. The cost is added to route information learned on this interface through RIP and is included in subsequent RIP packets sent to other interfaces. IPX discards the packet when its hop count exceeds a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network. For all non-WAN and HSSI interfaces, the default value translates into a tick cost of 1 in the routing table. For all WAN interfaces, the default value translates into a tick cost of 6 in the routing table.
Instructions:	Do not change the default value of this parameter unless you are an experienced IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value of this parameter can significantly affect router performance. If you are an experienced user, enter a value that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.38

Parameter: Host Number (hex)

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: None

Options: Any valid IPX host ID number

Function: If you enable the global Multiple Host Address Enable parameter and want to accept the PROM-based default setting for the MAC Address Select circuit parameter, this IPX interface adopts a host number based on the MAC address of the underlying circuit. In this case, a PROM on the circuit supplies the number for the MAC address of the circuit and the host number of the interface.

You can enter a host number for this interface when:

- The Multiple Host Addressing parameter is enabled.
- You do not want to accept the default PROM-based setting for the MAC Address Select parameter.
- The circuit type supports only selective mode of operation (such as with Ethernet circuits).

If you enter a host number, the circuit adopts that value as the MAC address at which this interface can receive frames. (The MAC address configured at the circuit/line level remains in effect for all other interfaces configured on the same circuit.)

You can enter a host number for this interface when the underlying circuit is token ring; see the instructions that follow.

Site Manager does not let you enter an IPX host number for any IPX interface if you disable the Multiple Host Address Enable parameter in the IPX Global Parameters window.

Instructions: Enter a value only if the circuit is not token ring and you want to assign a host number to this IPX interface that is unique within the IPX internetwork.

To set the host number of an IPX interface on a token ring circuit, you must change the MAC Address Select parameter for that circuit to CNFG (user-configured) and enter a MAC Address Override value for the circuit. The interface uses that value as its host number. This changes the circuit MAC address for all protocols configured on that token ring circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.25

Parameter: **Configured Encaps**

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: Circuit media dependent

Options: Ethernet │ LSAP │ Novell │ SNAP │ PPP

Function: Specifies the encapsulation methods (such as Ethernet, PPP, Novell, LSAP, or SNAP) available for each circuit type (such as Ethernet, token ring, or synchronous). The encapsulation method supports communication on a specific logical network.

Instructions: Select an encapsulation method that matches the one the clients and servers on the same logical network use and is appropriate for the physical circuit, as follows:

Ethernet circuits support Ethernet, LSAP, Novell, and SNAP frames.

Token ring circuits support LSAP and SNAP frames.

Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21, T1/E1) support SNAP, PPP, and X.25 Point-to-Point (Ethernet) frames.

FDDI circuits support LSAP and SNAP frames.

HSSI circuits support PPP and SNAP frames.

ISDN circuits support PPP frames.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.40

Parameter: **TR End Station**

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: Disable

Options: Enable │ Disable

Function: Enables or disables source routing on this interface. This parameter appears only when you add an IPX interface on a token ring circuit.

Instructions: Select Enable if this interface connects to a bridged token ring network. Select Disable only if you want to disable source routing over this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.59

Parameter: NetBIOS Accept

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: Disable

Options: Enable | Disable

Function: Enables or disables acceptance of all NetBIOS Type 20 (broadcast) packets received by this interface from an external source.

Instructions: Select Enable if you want this interface to accept all NetBIOS broadcast packets from an external source. Select Disable if you want this interface to reject all NetBIOS broadcast packets from an external source.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.60

Parameter: NetBIOS Deliver

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: Disable

Options: Enable | Disable

Function: Enables or disables outbound delivery of all NetBIOS Type 20 (broadcast) packets received by this interface from another interface.

Instructions: Select Enable if you want to enable outbound delivery of NetBIOS broadcast packets received internally. Select Disable to drop NetBIOS broadcast packets received internally.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.61

Parameter: **FR Broadcast (hex)**

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: 0xFFFFFFFFFFFF (not displayed)

Options: Default value or a user-specified WAN broadcast address

Function: Specifies a broadcast address for this IPX interface. (This parameter is available for any WAN protocol and any media type.)

The default value (0xFFFFFFFFFFFF) causes the data link layer to issue a WAN broadcast packet on all active virtual circuits. The value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol.

Instructions: Leave blank to accept the default value or enter a WAN broadcast address to send all broadcast traffic through the IPX interface you are configuring. With the default value, the IPX router sends all broadcast traffic through all logical connections associated with the IPX interface you are configuring. Broadcast traffic includes RIP and SAP broadcasts.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.28

Parameter: **FR Multicast (hex)**

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: 0xFFFFFFFFFFFF (not displayed)

Options: Default value or a user-specified WAN multicast address

Function: Specifies a multicast address for this IPX interface. (This parameter is available for any WAN protocol and any media type.)

The default value (0xFFFFFFFFFFFF) causes the data link layer to issue a multicast packet on all active virtual circuits. The value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol.

Instructions: Leave blank to accept the default value or enter a WAN multicast address to send all multicast traffic through the IPX interface you are configuring. With the default value, the IPX router sends all multicast traffic through all logical connections associated with the IPX interface you are configuring.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.30

Parameter: **IPX Watchdog Spoofing**

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: Disable

Options: Enable | Disable

Function: Specifies whether a router can respond locally to broadcast IPX watchdog packets on behalf of clients that use dial-in connections. When you enable this parameter you also enable SPX keepalive spoofing.

Instructions: Enable local watchdog packet acknowledgment to improve the efficiency of IPX wide area links.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.64

Parameter: **Delay**

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: 0

Options: 0 to 2147483647

Function: Specifies the length of time, in microseconds, required to transmit 1 byte of data (excluding protocol headers) to a destination on the other end of this IPX circuit if the circuit is free of other traffic.

Instructions: Enter a value from 0 to 2147483647.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.66

Parameter: **Stabilization Timer Delay (secs)**

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: 0

Options: 0 to 2147483647

Function: Determines the amount of time, in seconds, that RIP/SAP waits before sending out initial route information when the dial-on-demand route first becomes enabled.

Instructions: The more routes that you expect a router to handle or the more dynamic the network is, the higher you should set this value to allow the router enough time to assimilate incoming routes before it sends out an initial update on a circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.69

Parameter:	**Throughput**
Path:	Configuration Manager > Protocols > IPX > Interfaces
Default:	0
Options:	0 to 2147483647
Function:	Specifies the amount of data, in bits per second, that can flow through an IPX circuit if the circuit is free of other traffic.
Instructions:	Enter a value between 0 and 2147483647.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.67

Parameter:	**FR SVC Broadcast**
Path:	Configuration Manager > Protocols > IPX > Interfaces
Default:	Disable
Options:	Enable | Disable
Function:	Determines whether frame relay SVCs should be established for all adjacent hosts before sending RIP and SAP updates.
Instructions:	Select Enable to establish SVCs for all adjacent hosts before sending RIP and SAP updates. Otherwise, select Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.70

IPX Change Circuit Parameters

IPX change circuit parameters modify the way IPX runs over a particular circuit. You access these parameters in the IPX Change Circuit window (Figure B-6) for each circuit that you configured.

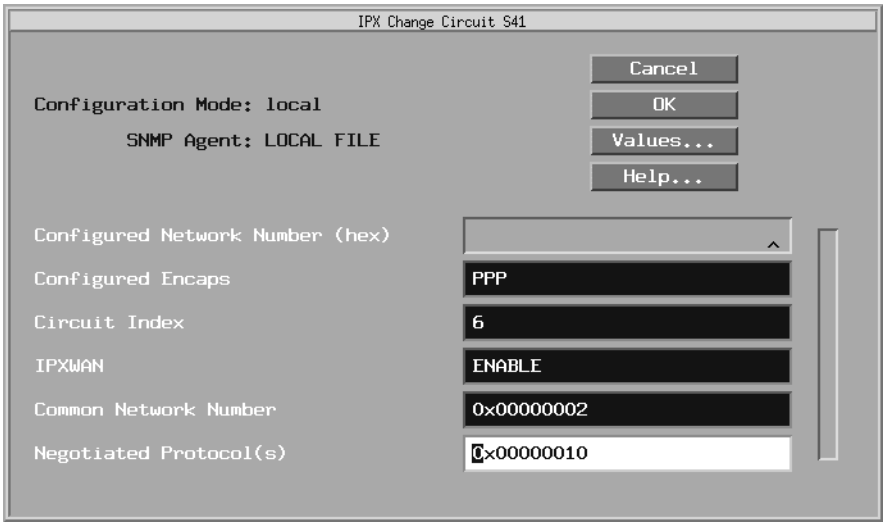

Figure B-6. IPX Change Circuit Window

Parameter: Configured Network Number (hex)

Path: Configuration Manager > Protocols > IPX > Interfaces > Circuit > Change

Default: None

Options: Any valid IPX network number in hexadecimal format

Function: Identifies the IPX network number assigned to this IPX circuit. This parameter is active only for circuits that are not configured as IPXWAN interfaces or for those with the IPXWAN parameter explicitly disabled.

Instructions: Enter a valid IPX network number in hexadecimal notation.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.22

Note: The Configured Network Number parameter is active only for circuits that are not configured as IPXWAN interfaces. The IPXWAN, Common Network Number, and Negotiated Protocol(s) parameters appear only when the circuit is configured as an IPXWAN interface.

Parameter: Configured Encaps

Path: Configuration Manager > Protocols > IPX > Interfaces > Circuit > Change

Default: Circuit media dependent

Options: Ethernet │ LSAP │ Novell │ SNAP │ PPP

Function: Specifies the encapsulation method (such as Ethernet, PPP, Novell, LSAP, or SNAP) available for each circuit type (such as Ethernet, token ring, or sync). The encapsulation method supports communication on a specific logical network.

Instructions: Select an encapsulation method that matches the one the clients and servers on the same logical network use and is appropriate for the physical circuit, as follows:

- Ethernet circuits support Ethernet, LSAP, Novell, and SNAP frames.
- Token ring circuits support LSAP and SNAP frames.
- Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21, T1/E1) support SNAP, PPP, and X.25 Point-to-Point (Ethernet) frames.
- FDDI circuits support LSAP and SNAP frames.
- HSSI circuits support PPP and SNAP frames.
- ISDN circuits support PPP frames.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.40

Parameter: Circuit Index

Path: Configuration Manager > Protocols > IPX > Interfaces > Circuit > Change

Default: System-assigned

Options: Any valid circuit identifier

Function: Uniquely identifies this circuit within this instance of IPX.

Instructions: Accept the default or enter a valid circuit identifier.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.6

Parameter:	**IPXWAN**
Path:	Configuration Manager > Protocols > IPX > Interfaces > Circuit > Change
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables IPXWAN for this interface on the router. This parameter is active only for circuits that are configured as IPXWAN interfaces.
Instructions:	Select Enable to turn on IPXWAN negotiation for this interface. Select Disable to turn off IPXWAN negotiation for this interface.
MIB Object ID:	Not Applicable

Parameter:	**Common Network Number**
Path:	Configuration Manager > Protocols > IPX > Interfaces > Circuit > Change
Default:	None
Options:	Any valid IPX network number, 0x00000000 to 0xFFFFFFFD in hexadecimal format
Function:	Specifies the IPX common network number assigned to this IPX circuit. This parameter is active only for circuits that are configured as IPXWAN interfaces that have the IPXWAN parameter enabled.
Instructions:	Enter a valid IPX network number in hexadecimal format. Do not use the values 0xFFFFFFFE or 0xFFFFFFFF as network numbers. These values are reserved for system use.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.24

Parameter:	**Negotiated Protocol(s)**
Path:	Configuration Manager > Protocols > IPX > Interfaces > Circuit > Change
Default:	Unnumbered RIP
Options:	RIP | Unnumbered RIP
Function:	Indicates the protocol negotiated for this interface. This parameter is active only for circuits that are configured as IPXWAN interfaces and that have the IPXWAN parameter enabled.
Instructions:	Accept the default or click on Values to display the other choices. You can select more than one option. Click on the options you prefer, then click on OK to accept your choices. The parameter value appears as a hexadecimal number in the IPX Change Circuit window. The values are as follows: 0x00000008 -- RIP 0x00000010 -- Unnumbered RIP 0x00000018 -- RIP and Unnumbered RIP
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.8

IPX RIP Circuit Parameters

IPX RIP circuit parameters determine the way RIP behaves on a particular circuit. You access these parameters fin the IPX RIP Circuit window (Figure B-7). To view all parameters in this window, click on the scroll bar.

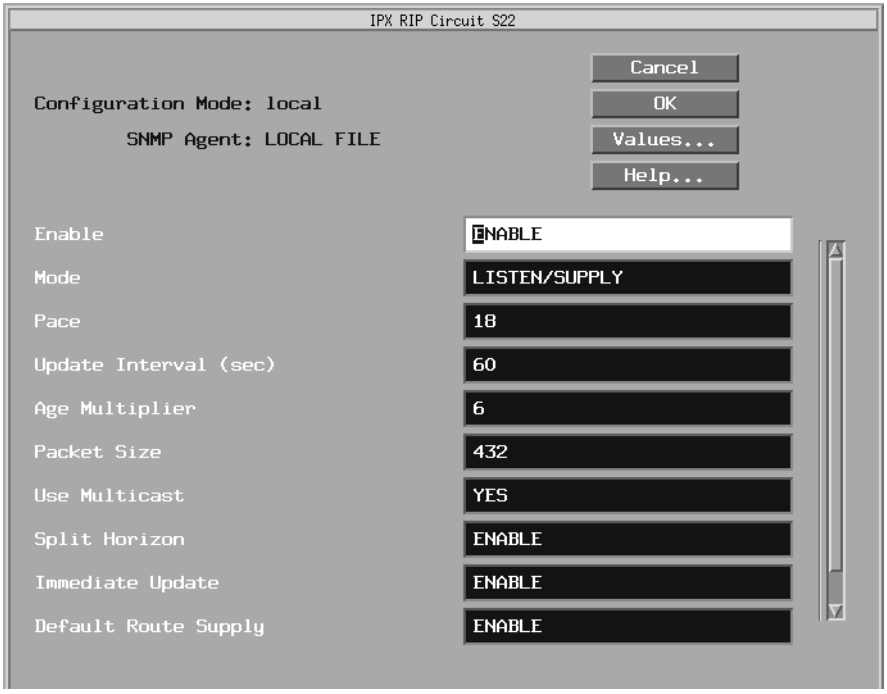

Figure B-7. IPX RIP Circuit Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Enable

Options: Enable | Disable

Function: Specifies whether RIP is enabled on this IPX circuit.

Instructions: Select Enable to enable RIP on this circuit. Select Disable to disable RIP on this circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.2

Note: If this parameter is set to Enable, a route filter can still prohibit the interface from updating its internal routing tables.

Parameter: Mode

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Listen/Supply

Options: Listen/Supply | Listen | Supply

Function: Specifies the mode for this circuit.

Instructions: Select one of the following values:

Listen/Supply -- specifies that this interface both listens for and supplies RIP updates.

Listen -- specifies that this interface listens to RIP periodic and triggered updates from neighboring networks and conveys received routing information to its internal routing table.

Supply -- specifies that the interface transmits all RIP periodic and triggered updates to routers in neighboring networks.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.6

Parameter: Pace

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP
Default: 18
Options: 0 to 1000
Function: Specifies the maximum pace (in packets per second) at which RIP packets can be sent on this circuit. A value of 0 means that there is no limit on the pace.
Instructions: Accept the default or specify an integer value up to 1000.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.7

Parameter: Update Interval (sec)

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP
Default: 60
Options: 0 to 2678400
Function: Adjusts the frequency of RIP update packet transmissions, in seconds, for this circuit.
Instructions: The higher the number you enter, the less frequent the transmissions. If you enter 0, no periodic RIP updates are sent out over the IPX interface to the router. However, RIP immediate (one-time) update packets still propagate through the network, in compliance with Novell standards.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.8

Parameter: Age Multiplier

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP
Default: 3
Options: 1 to 6
Function: Specifies the holding multiplier as the number of update intervals for information received in RIP periodic updates.
Instructions: Accept the default value or specify a value from 1 to 6. Increasing this value can cause routes to take longer to age out. Decreasing it can cause the router to age routes prematurely, if routing updates are missed. The combination of the update interval and age multiplier should be the same for all systems on a network segment.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.9

Parameter:	**Packet Size**
Path:	Configuration Manager > Protocols > IPX > Interfaces > RIP
Default:	432
Options:	Circuit-type dependent
Function:	Specifies the maximum RIP packet size, in bytes, used on this circuit.
Instructions:	Accept the default (432 bytes) unless you have a reason for specifying a different packet size. The packet size plus the IPX header (30 bytes) cannot exceed the MTU of the link.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.10

Parameter:	**Use Multicast**
Path:	Configuration Manager > Protocols > IPX > Interfaces > RIP
Default:	Yes
Options:	Yes | No
Function:	Specifies whether to use a multicast address, configured with the FR Multicast (hex) parameter, to send RIP packets.
Instructions:	Accept the default to allow multicast transmission of RIP packets. Select No to disable multicast transmission of RIP packets.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.14

Parameter: Split Horizon

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Enable

Options: Enable | Disable

Function: When generating RIP updates to be transmitted from an interface, the interface can exclude RIP routes learned on that interface.

Instructions: Select Enable if you previously set this parameter to Disable and now do not want the router to transmit RIP updates received from the interface over that same interface.

Select Disable only if you want the router to transmit RIP updates received from the interface over that same interface. Routes learned on that interface will be included in the RIP updates generated for that interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.15

Parameter: Immediate Update

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Enable

Options: Enable | Disable

Function: When a change in status occurs for this circuit, immediately propagate that information to other routers in the internetwork.

Instructions: Accept the default. Enabling this parameter facilitates network traffic by letting routers know immediately about new or failed routes. When this parameter is disabled, other routers learn about such changes only at the next periodic update interval.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.17

Parameter: Default Route Supply

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Disable

Options: Enable │ Disable

Function: If a default route exists in the routing table, this parameter specifies whether to advertise the default route, 0xFFFFFFFE, in RIP packets.

Instructions: Select Enable to enable default route supply (that is, to advertise the default route) on this circuit.

Select Disable to disable default route supply (that is, not advertise the default route) on this circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.18

Parameter: Default Route Listen

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Disable

Options: Enable │ Disable

Function: Specifies whether to accept the default route, 0xFFFFFFFE, in RIP packets received on this circuit.

Instructions: Select Enable to accept the default route in RIP packets on this circuit.

Select Disable to reject the default route in RIP packets on this circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.19

IPX SAP Circuit Parameters

IPX SAP circuit parameters determine the way SAP works on a particular circuit. You access these parameters in the IPX SAP Circuit window (Figure B-8).

Figure B-8. IPX SAP Circuit Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP
Default: Enable
Options: Enable | Disable
Function: Specifies whether SAP is enabled on this IPX circuit.
Instructions: Select Enable to enable SAP on this circuit; select Disable to disable it.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.2

Note: If this parameter is set to Enable, a SAP filter can still prohibit the interface from updating its internal SAP tables. See the description of SAP filtering in Chapter 6, "Customizing IPX."

Parameter: Mode

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: Listen/Supply

Options: Listen/Supply | Listen | Supply

Function: Specifies the mode for this circuit.

Instructions: Select one of the following values:

Listen/Supply -- specifies that this interface both listens for and supplies SAP updates.

Listen -- specifies that this interface listens to SAP periodic and triggered updates from neighboring networks and conveys received SAP services information to its internal SAP services table.

Supply -- specifies that the interface transmits all SAP periodic and triggered updates to routers in neighboring networks.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.6

Parameter: Pace

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: 18

Options: 0 to 1000

Function: Specifies the maximum pace (in packets per second) at which SAP packets can be sent on this circuit. A value of 0 means that there is no limit on the pace.

Instructions: Accept the default, or specify an integer value up to 1000.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.7

Parameter: Update Interval (sec)

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: 60

Options: 0 to 2678400

Function: Adjusts the frequency, in seconds, of SAP update packet transmissions for this circuit.

Instructions: The higher the number you enter, the less frequent the transmissions. If you enter 0, no periodic updates are sent out over the IPX interface to the router. However, SAP immediate (one-time) updates still propagate through the network, in compliance with Novell standards.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.8

Parameter: Age Multiplier

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: 3

Options: 1 to 6

Function: Specifies the holding multiplier, in update interval increments, for information received in SAP periodic updates.

Instructions: Accept the default value or specify a value from 1 to 6. Increasing this value can cause routes to take longer to age out. Decreasing it can cause the router to age routes prematurely, if routing updates are missed. The combination of the update interval and age multiplier should be the same for all systems on a network segment.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.9

Parameter: **Packet Size**

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: 480

Options: Circuit-type dependent

Function: Specifies the maximum SAP packet size, in bytes, used on this circuit.

Instructions: Accept the default (480 bytes) unless you have a reason for specifying a different packet size. The packet size plus the IPX header (30 bytes) cannot exceed the MTU of the link.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.10

Parameter: **Nearest Server Reply**

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: Yes

Options: Yes | No

Function: Specifies whether to respond to SAP get_nearest_server requests.

Instructions: Accept the default to allow this router to respond to a SAP get_nearest_server request. If you have disabled split horizon, you may want to set this parameter to No.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.11

Parameter: **Use Multicast**

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: Yes

Options: Yes | No

Function: Specifies whether to use a multicast address to send SAP packets.

Instructions: Accept the default to allow multicast transmission of SAP packets. Select No to disable multicast transmission of SAP packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.16

Parameter: Save Full Name

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: Yes

Options: Yes | No

Function: Determines whether the router will save all 48 bytes in the service name field of SAP packets or ignore all characters after the null character when a service field name is less than 48 bytes long.

Instructions: Accept the default to save all 48 bytes in the service name field of SAP packets. Select No to ignore all characters after the null character.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.20

Parameter: Split Horizon

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: Enable

Options: Enable | Disable

Function: When generating SAP updates to be transmitted from an interface, the interface can exclude SAP servers learned on that interface.

Instructions: Select Enable if you previously set this parameter to Disable and now do not want the router to transmit SAP updates received from the interface over that same interface.

Select Disable only if you want the router to transmit SAP updates received from the interface over that same interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.17

Parameter:	**Immediate Update**
Path:	Configuration Manager > Protocols > IPX > Interfaces > SAP
Default:	Enable
Options:	Enable | Disable
Function:	When a change in status occurs for this circuit, immediately propagate that information to other routers in the internetwork.
Instructions:	Accept the default. Enabling this parameter facilitates network traffic by letting routers know immediately about new or failed services. When this parameter is disabled, other routers learn about such changes only at the next periodic update interval.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.33.1.19

IPX NetBIOS Static Route Configuration Parameters

IPX NetBIOS static route configuration parameters establish a NetBIOS static route. You access these parameters in a the IPX NetBIOS Static Route Configuration window (Figure B-9).

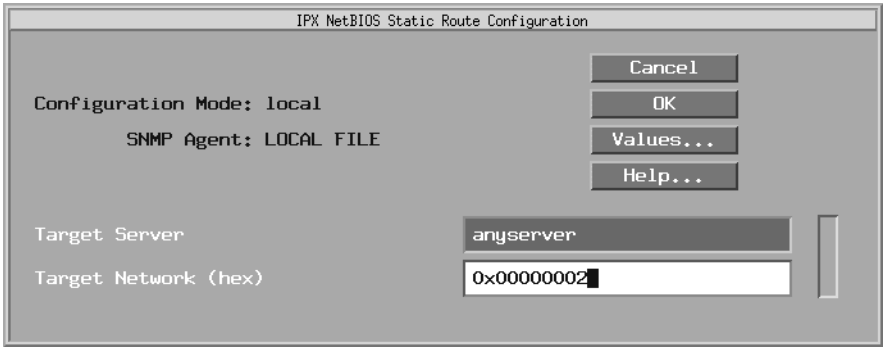

Figure B-9. IPX NetBIOS Static Route Configuration Window

Parameter: Target Server

Path: Configuration Manager > Protocols > IPX > NetBIOS Static Routes > Add

Default: None

Options: The name of a NetBIOS target server, specified as a string of up to 16 alphanumeric characters (which can include wildcards and pattern-matching characters). You can include any printable character, including $, #, and so on. To specify a backslash (\), enter two backslashes (\\). You can also use the hexadecimal equivalent (*xx*) of any valid ASCII character. For example, you can specify \20 for space or \21 for ! (note that *xx* counts as one character).

Function: Specifies the name of the NetBIOS server.

Instructions: Enter the name or part of the name of the NetBIOS server. The name can be up to 16 alphanumeric characters. For a list of the wildcards and pattern-matching characters, see Table 6-1 on page 5-129.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.27.1.4

Note: The Configuration Manager does not let you reconfigure the Target Server parameter for a static route. If you want to change this parameter, you must delete the static route and add a new route. However, you can reconfigure all other parameters associated with a static route..

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > NetBIOS Static Routes > Add

Default: None

Options: Any valid network address in hexadecimal notation

Function: Specifies the address of a destination network that you want to receive NetBIOS broadcast packets destined for the specified target server.

Instructions: Enter a network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.27.1.5

IPX NetBIOS Static Route Parameters

IPX NetBIOS static route parameters determine the location of a NetBIOS static route.You access these parameters in the IPX NetBIOS Static Routes window (Figure B-10).

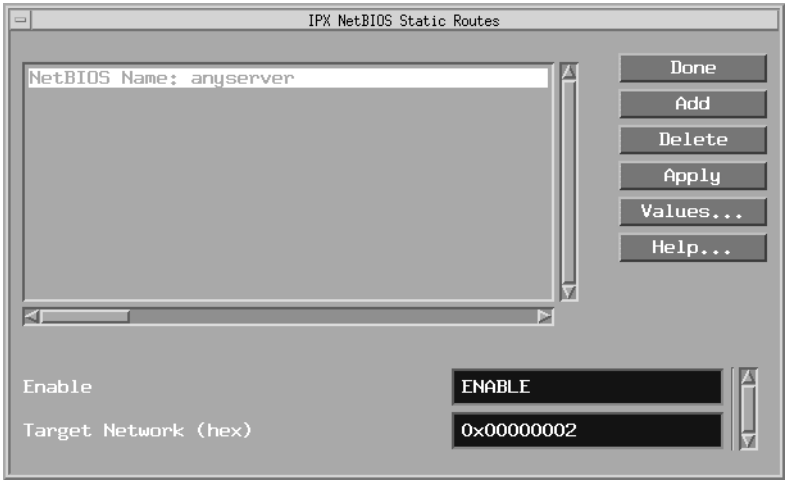

Figure B-10. IPX NetBIOS Static Routes Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > NetBIOS Static Routes

Default: Enable

Options: Enable | Disable

Function: Specifies the state (active or inactive) of the static route record in the NetBIOS routing table.

Instructions: Select Disable to make the static route record inactive in the NetBIOS routing table. Select Enable to make the static route record active in the NetBIOS routing table.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.27.1.2

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > NetBIOS Static Routes

Default: None

Options: Any valid network address in hexadecimal notation

Function: Specifies the address of a destination network that you want to receive NetBIOS broadcast packets destined for the specified target server.

Instructions: Enter a network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.27.1.5

Adjacent Host Configuration Parameters

IPX adjacent host configuration parameters establish an adjacent host. You access these parameters in the IPX Adjacent Host Configuration window (Figure B-11).

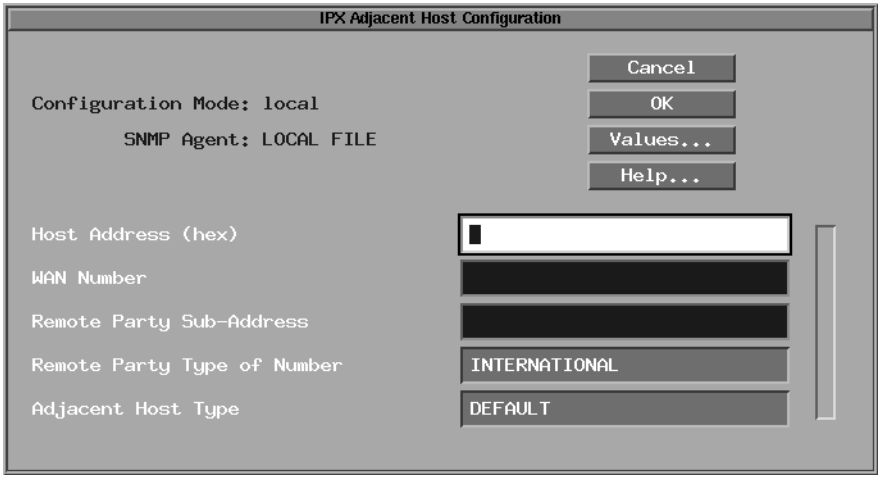

Figure B-11. IPX Adjacent Host Configuration Window

Parameter: Host Address (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts > Add

Default: None

Options: Valid host ID of the adjacent host

Function: Specifies the host ID of the adjacent host.

Instructions: Enter a host ID of up to 12 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.5

Parameter: WAN Number

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts > Add

Default: None

Options: WAN Address | Data Link Connection Identifier | X.25 PVC Logical Channel Number

Function: Lets you enter a WAN address, DLCI, or X.25 PVC logical channel number. The format depends on the underlying data link protocol type.

Instructions: Enter a WAN address of up to 16 hexadecimal characters if the interface is on an ATM or SMDS network. Enter a decimal DLCI number if the interface is on a frame relay network. Enter an X.121 address if the interface is on an X.25 switched virtual circuit. Enter a logical channel number if the interface is on an X.25 permanent virtual circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.6

Parameter: Remote Party Sub-Address

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts > Add

Default: None

Options: 8-digit hexadecimal number

Function: Establishes a switched virtual circuit (SVC) connection to the adjacent host.

Instructions: Supply the address, in hexadecimal format, of the remote party.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.7

Parameter: Remote Party Type of Number

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts > Add

Default: International

Options: Unknown | International

Function: Specifies the type of number used to establish a switched virtual circuit (SVC) connection to the adjacent host.

Instructions: Accept the default. Otherwise, select Unknown.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.8

Parameter: Adjacent Host Type

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts > Add

Default: Default

Options: Default | Frame Relay (E.164) | Frame Relay (X.121) | Frame Relay (DLCI)

Function: Specifies the type of static host used when establishing a switched virtual circuit (SVC) connection to the adjacent host.

Instructions: Specify the type of static host.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.9

IPX Adjacent Hosts Parameters

IPX adjacent hosts parameters determine the location of an adjacent host. You access these parameters in the IPX Adjacent Hosts window (Figure B-12).

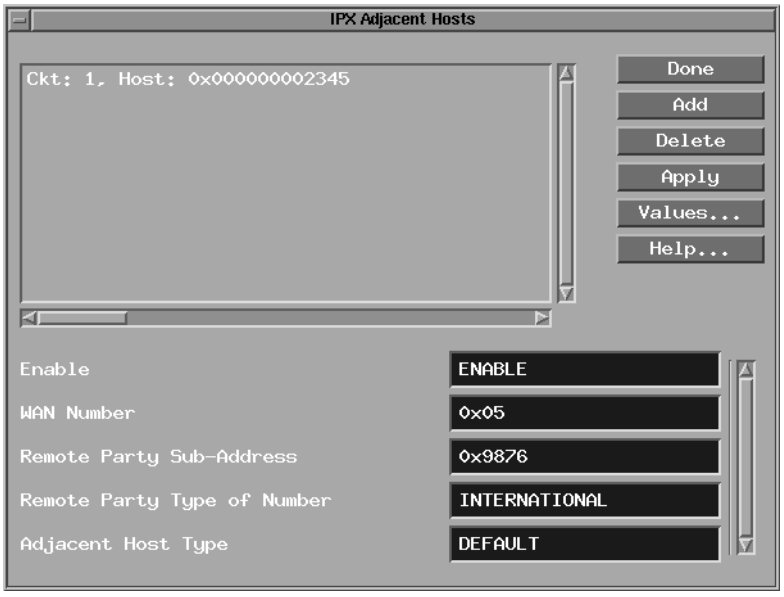

Figure B-12. IPX Adjacent Hosts Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts

Default: Enable

Options: Enable | Disable

Function: Sets the state (active or inactive) of the adjacent host record in the IPX host tables.

Instructions: Select Disable to make the adjacent host record inactive in the IPX host table.

Select Enable to make the adjacent host record active in the IPX host table.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.2

Parameter:	**WAN Number**
Path:	Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts > Add
Default:	None
Options:	WAN Address | Data Link Connection Identifier | X.25 PVC Logical Channel Number
Function:	Lets you enter a WAN address, DLCI, or X.25 PVC logical channel number. The format depends on the underlying data link protocol type.
Instructions:	Enter a WAN address of up to 16 hexadecimal characters if the interface is on an ATM or SMDS network. Enter a decimal DLCI number if the interface is on a frame relay network. Enter an X.121 address if the interface is on an X.25 switched virtual circuit. Enter a logical channel number if the interface is on an X.25 permanent virtual circuit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.26.1.6

Parameter: Remote Party Sub-Address

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts > Add

Default: None

Options: Eight-digit hexadecimal number

Function: Establishes a switched virtual circuit (SVC) connection to the adjacent host.

Instructions: Supply the address, in hexadecimal format, of the remote party.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.7

Parameter: Remote Party Type of Number

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts > Add

Default: International

Options: Unknown | International

Function: Specifies the type of number used to establish a switched virtual circuit (SVC) connection to the adjacent host.

Instructions: Accept the default. Otherwise, select Unknown.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.8

Parameter: Adjacent Host Type

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts > Add

Default: Default

Options: Default | Frame Relay (E.164) | Frame Relay (X.121) | Frame Relay (DLCI)

Function: Specifies the type of static host used when establishing a switched virtual circuit (SVC) connection to the adjacent host.

Instructions: Specify the type of static host.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.9

IPX Static Route Configuration Parameters

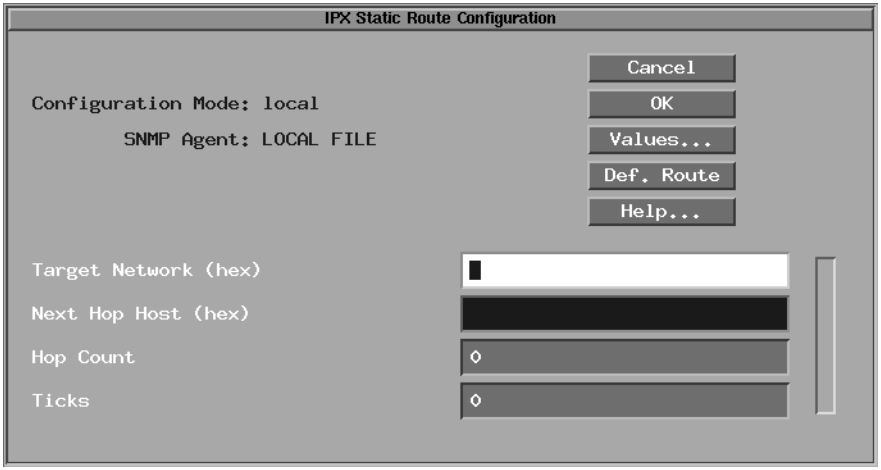

Figure B-13. IPX Static Route Configuration Window

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route > Add

Default: None

Options: Any valid network address in hexadecimal notation

Function: Specifies the address of the network to which you want to configure the static route.

Instructions: Enter a network address of up to 8 hexadecimal characters or click on Def. Route to have the Configuration Manager fill in the default route 0xFFFFFFFE.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.5

Note: The Configuration Manager does not let you reconfigure the Target Network parameter for a static route. If you want to change this parameter, you must delete the static route and add a new route with the proper information. However, you can reconfigure all other parameters associated with a static route.

Parameter: Next Hop Host (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route > Add

Default: None

Options: Any valid host address in hexadecimal notation

Function: Specifies the address of the next-hop host in the static routing path.

Instructions: Enter a host address of up to 12 hexadecimal characters. The next-hop host address is the MAC address of the next hop on the way to the destination.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.8

Parameter: Hop Count

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route > Add

Default: 0

Options: 0 to the value of the Maximum Hops parameter minus 1

Function: The IPX router uses the hop count when determining the best route for a datagram to follow. The hop count is also propagated through RIP. The default setting of 0 for static routes means “use the hop count associated with the interface.”

Instructions: Accept the default (0) or enter a value from 1 to one less than the maximum number of hops.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.7

Parameter:	**Ticks**
Path:	Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route > Add
Default:	0
Options:	0 to maximum positive integer
Function:	Specifies the number of 1/18th-second timer ticks required for an IPX datagram to traverse this static route. The IPX router uses tick cost when determining the best route for a datagram to follow. The tick cost is also propagated through RIP. The default setting of 0 for the tick cost of static routes means “use the tick count associated with the interface.”
Instructions:	Accept the default value (0) or enter a value from 1 to the maximum positive integer.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.19.1.6

IPX Static Route Parameter Descriptions

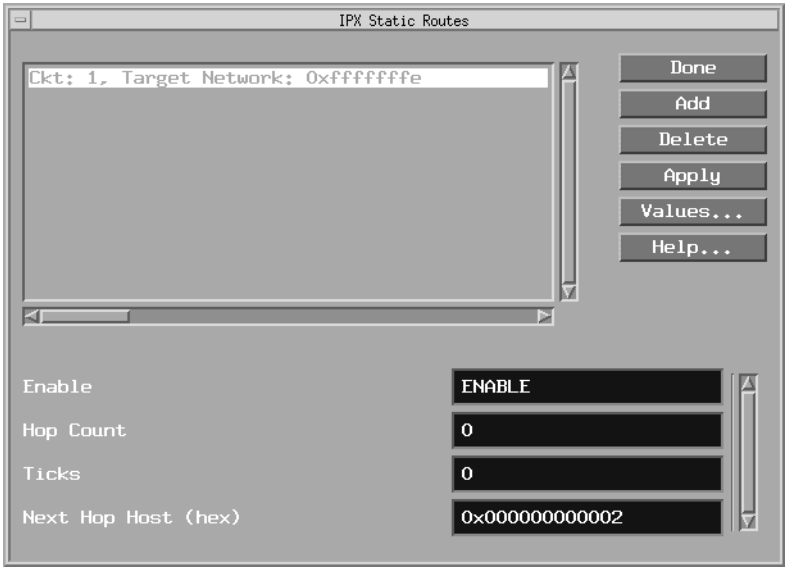

Figure B-14. IPX Static Routes Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route

Default: Enable

Options: Enable | Disable

Function: Specifies the state (active or inactive) of the static route record in the IPX routing tables.

Instructions: Select Disable to make the static route record inactive in the IPX routing table.

Select Enable to make the static route record active in the IPX routing table.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.2

Parameter: Hop Count

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route

Default: 0

Options: 0 to the value of the Maximum Hops parameter minus 1

Function: The IPX router uses the hop count when determining the best route for a datagram to follow. The hop count is also propagated through RIP. The default setting of 0 for static routes means “use the hop count associated with the interface.”

Instructions: Accept the default (0) or enter a value from 1 to one less than the maximum number of hops.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.7

Parameter: Ticks

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route

Default: 0

Options: 0 to maximum positive integer

Function: Specifies the number of 1/18th-second timer ticks required for an IPX datagram to traverse this static route. The IPX router uses tick cost when determining the best route for a datagram to follow. The tick cost is also propagated through RIP. The default setting of 0 for the tick cost of static routes means “use the tick count associated with the interface.”

Instructions: Accept the default value (0) or enter a value from 1 to the maximum positive integer.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.6

Parameter: Next Hop Host (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route

Default: None

Options: Any valid host address in hexadecimal notation

Function: Specifies the address of the next-hop host in the static routing path.

Instructions: Enter a next-hop host address of up to 12 hexadecimal characters. The next-hop host address is the MAC address of the next hop on the way to the destination.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.8

IPX Static Service Configuration Parameters

This section describes all parameters shown in the IPX Static Services Configuration window (Figure B-15).

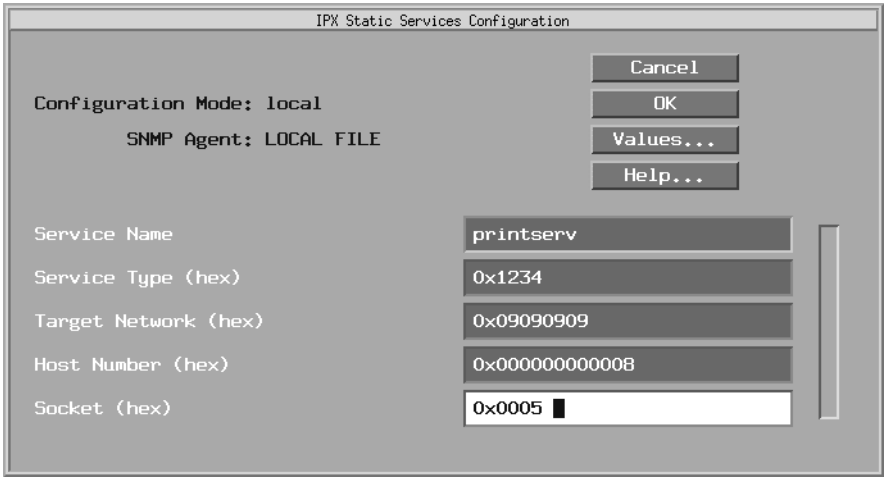

Figure B-15. IPX Static Services Configuration Window

Parameter: Service Name

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv. > Add

Default: None

Options: Any valid Novell NetWare server name

Function: Assigns a symbolic name to the service you want to advertise.

Instructions: Use the *actual* name of the server that the clients will attach to. Make this name meaningful to the network administrator. The name must be unique among all names assigned to IPX servers of the same type on the IPX internetwork.

See the documentation that came with your NetWare operating system for guidelines on specifying a server name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.5

Parameter: **Service Type (hex)**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv. > Add

Default: None

Options: Any valid Novell server type number in 4-digit hexadecimal format. (The number must be a value between 0x0001 and 0xFFFE, inclusive.)

Function: Specifies the type of service to advertise from the associated IPX (LAN) interface (for example, 0x0004 for file server, 0x0007 for printer server).

Instructions: Enter the server type number in 4-digit hexadecimal format. Include leading zeros.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.6

Parameter: **Target Network (hex)**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv. > Add

Default: None

Options: Any valid IPX network address in hexadecimal notation

Function: Specifies the network address of this service.

Instructions: Enter a network address of up to 8 hexadecimal characters. The path to the network you specify for this service must exist as an entry in the IPX routing table. The entry can be learned dynamically by the router, or you can configure the entry as a static route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.7

Parameter: Host Number (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv. > Add

Default: None

Options: The address (host ID) of the service

Function: Specifies the address of a remote IPX host (a NetWare server) that can provide local clients with specific NetWare services, such as file, print, gateway, or terminal server services.

Instructions: Enter a string of up to 12 hexadecimal characters (6 bytes) as the address (host ID) of the remote IPX host/server. (For example, most NetWare server host IDs are usually 0x000000000001.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.8

Parameter: Socket (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Add

Default: None

Options: Any valid socket address from 0x0001 to 0xFFFE.

Function: Specifies the socket address of this service.

Instructions: Enter any valid socket address consisting of up to 4 hexadecimal characters (for example, 0x0451).

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.9

Note: See Appendix D, "Common Service Types and Identifiers for a list of common service types.

IPX Static Service Parameters

This section describes all parameters shown in the IPX Static Services window (Figure B-16).

Note: The Configuration Manager does not let you change the Service Name or Type parameters you set when you add a static service. To establish new values for these parameters for a particular static service, you must delete that service and configure a new service. You can, however, reconfigure all other parameters associated with a static service.

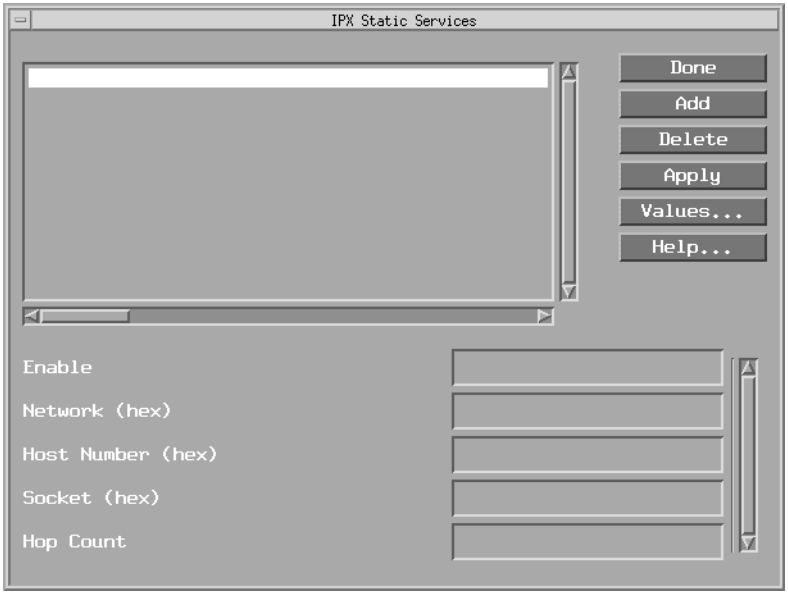

Figure B-16. IPX Static Services Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv

Default: Enable

Options: Enable | Disable

Function: Enables or disables a static service previously added to a specific IPX interface.

Instructions: Select Enable to reenable a static service previously disabled. This restores client access to NetWare services configured earlier on the IPX interface.

Disable a static service to make NetWare services configured earlier unavailable to clients.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.2

Parameter: Network (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv

Default: None

Options: Any valid IPX network address in hexadecimal notation

Function: Specifies the network address of this service.

Instructions: Enter a network address of up to 8 hexadecimal characters. The path to the network you specify for this service must exist as an entry in the IPX routing table. The entry can be learned dynamically by the router, or you can configure the entry as a static route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.7

Parameter: Host Number (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv

Default: None

Options: The address (host ID) of the service

Function: Specifies the address of a remote IPX host (a NetWare server) that can provide local clients with specific NetWare services, such as file, print, gateway, or terminal server services.

Instructions: Enter a string of up to 12 hexadecimal characters (6 bytes) as the address (host ID) of the remote IPX host/server.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.8

Parameter: Socket (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv
Default: None
Options: Any valid socket address from 0x0001 to 0xFFFE
Function: Specifies the socket address of this service.
Instructions: Enter any valid socket address consisting of up to 4 hexadecimal characters.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.9

Parameter: Hop Count

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv
Default: None
Options: Any valid number of hops, from 1 to the value of the Maximum Hops parameter minus 1
Function: Specifies the number of subsequent router hops required from this router to reach a specific remote Novell server or service.
Instructions: Enter the number of router hops that exist between the router and the service you want to advertise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.12.1.10

Route Filter Configuration Parameters

This section describes all parameters shown in the IPX Route Filter Configuration window (Figure B-17).

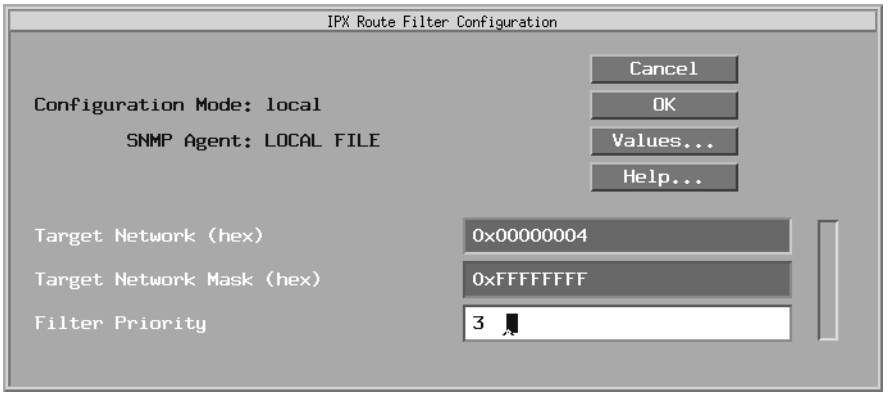

Figure B-17. IPX Route Filter Configuration Window

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Table > Route Filter > Add

Default: None

Options: Any valid NetWare address in hexadecimal format

Function: Identifies the network on which you want to apply the filter.

Instructions: Enter the address of the target network in hexadecimal format. Using a mask, you can make this stand for a single filter ID or for a range of IDs with similar addresses. You can select all addresses by entering the wildcard value 0xFFFFFFFF.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.6

Parameter: Target Network Mask (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Table > Route Filter > Add

Default: None

Options: 0x00000000 to 0xFFFFFFFF

Function: Specifies the mask that you want to apply.

Instructions: Enter 8 hexadecimal characters.

The character F in the mask definition requires an exact match with the corresponding character in the filter ID.

The mask character 0 matches any alphanumeric character.

You can combine the F and 0 characters in any order in the mask to filter any combination of network addressing schemes used within the IPX internetwork.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.7

Parameter: Filter Priority

Path: Configuration Manager > Protocols > IPX > Static/Filter Table > Route Filter > Add

Default: None

Options: 0 to the maximum positive integer

Function: Specifies the priority of this filter in relation to other filters of the same type.

Instructions: Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.13

IPX Route Filter Parameters

This section describes all the parameters in the IPX Route Filters window (Figure B-18).

Figure B-18. IPX Route Filters Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Static/Filter Table > Route Filter
Default: Enable
Options: Enable | Disable
Function: Enables or disables a route filter previously added to a specific IPX interface.
Instructions: Select Disable to disable a route filter. Select Enable to reenable a route filter.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.2

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Route Filter

Default: None

Options: Any valid NetWare address in hexadecimal format

Function: Identifies the network on which you want to apply the filter.

Instructions: Enter the address of the target network in hexadecimal format. Using a filter, you can make this stand for a single ID or for a range of IDs with similar addresses. You can select all addresses by entering the wildcard value 0xFFFFFFFF.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.6

Parameter: Target Network Mask (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Route Filter

Default: None

Options: 0x00000000 to 0xFFFFFFFF

Function: Specifies the mask that you want to apply.

Instructions: Enter 8 hexadecimal characters.

The character F in the mask definition requires an exact match with the corresponding character in the filter ID.

The mask character 0 (zero) matches any alphanumeric character.

You can combine the F and 0 characters in any order in the mask to filter any combination of network addressing schemes used within the IPX internetwork.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.7

Parameter: Filter Priority

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Route Filter
Default: None
Options: 0 to the maximum positive integer
Function: Specifies the priority of this filter in relation to other filters of the same type.
Instructions: Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.13

Parameter: Mode

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Route Filter
Default: Outbound
Options: Outbound | Inbound | Both
Function: Specifies whether you want to apply the filter to inbound packets, outbound packets, or both.
Instructions: Specify Inbound if you want to apply the filter to RIP packets coming into this interface. Specify Both if you want to filter both inbound and outbound packets.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.8

Parameter: Protocol

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Route Filter
Default: Any
Options: Any | Local | RIP | Static
Function: Applies this filter only to routes learned from the specified protocol when sending RIP updates. This does not apply to inbound route filters.
Instructions: Specify the protocol on which you want to apply the filter.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.10

Parameter:	**Action**
Path:	Configuration Manager > Protocols > IPX > Static/Filter Table > Route Filter
Default:	Advertise/Accept
Options:	Advertise/Accept | Suppress
Function:	Specifies how to process any RIP advertisement that matches the route filter criteria you established.
Instructions:	Select Advertise/Accept to enable the filter to allow advertisement and acceptance of routes that match the specified route filter criteria. Select Suppress to configure the IPX router to drop RIP advertisements that match the specified route filter criteria.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.9

Parameter: Cost

Path: Configuration Manager > Protocols > IPX > Static/Filter Table > Route Filter

Default: 1 (for hop- or tick-based routing)

Options: 1 to maximum positive integer (if tick-based routing is enabled)

1 to one less than the value specified in the Maximum Hops parameter (if hop-based routing is enabled)

Function: Used only when the Action parameter is Advertise/Accept, this parameter assigns a cost for routes matching this filter. A zero cost indicates that the route's actual cost should be used. This parameter sets the cost (number of ticks or hops) for this interface. The cost is included in subsequent RIP packets sent to other interfaces. IPX drops the packet when its hop count exceeds a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network.

If the filter is an *inbound* filter, the entered cost replaces the cost associated with the route in the RIP advertisement, and the router uses this cost in its calculations.

If this is an *outbound* filter, the entered cost replaces the route's cost that this router advertises in RIP packets.

Instructions: Do not change the default value of this parameter unless you are an experienced IPX user. Changing the value of this parameter can significantly affect router performance. If you are an experienced user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.11

Service Network Filter Configuration Parameters

This section describes all parameters shown in the IPX Service Network Filter Configuration window (Figure B-19).

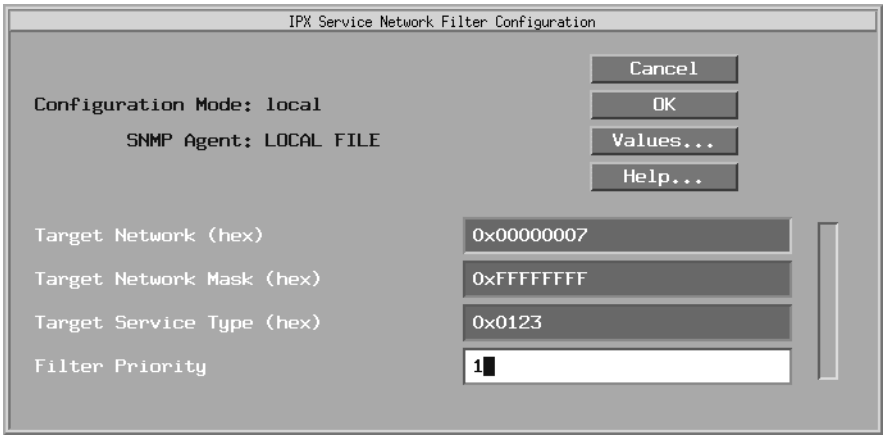

Figure B-19. IPX Service Network Filter Configuration Window

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter > Add

Default: None

Options: Any valid network address in hexadecimal notation

Function: Specifies the network that you want to filter. The value 0xFFFFFFFF specifies all networks.

Instructions: Enter a network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.6

Parameter: **Target Network Mask (hex)**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter > Add

Default: None

Options: Any valid IPX network address in hexadecimal notation

Function: The mask, combined with the Target Network parameter value, determines which networks will be filtered.

Instructions: Enter a network address or filter pattern of up to 8 hexadecimal characters. A mask of 0xFFFFFFFF specifies an exact match with the network address specified in the Target Network parameter. You can specify all networks by entering a Target Network of 0xFFFFFFFF and a Target Network Mask of 0xFFFFFFFF.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.7

Parameter: **Target Service Type (hex)**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter > Add

Default: None

Options: Any valid Novell server type number in 4-digit hexadecimal format

Function: Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.

Instructions: Enter the server type number in 4-digit hexadecimal format. Include leading zeroes. For all types, enter a value of 0xFFFF. See Appendix D, “Common Service Types and Identifiers for a list of valid server types.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.8

Parameter:	**Filter Priority**
Path:	Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter > Add
Default:	None
Options:	0 to the maximum number of filters of this type.
Function:	Specifies the priority of this filter in relation to other filters of the same type.
Instructions:	Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.14

IPX Service Network Filter Parameters

This section describes all parameters shown in the IPX Service Network Filters window (Figure B-20).

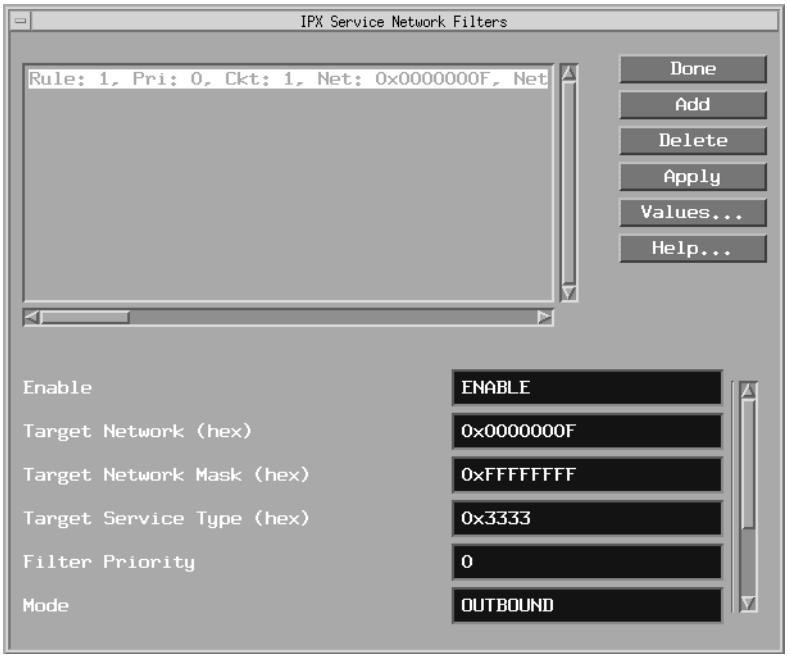

Figure B-20. IPX Service Network Filters Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: Enable

Options: Enable | Disable

Function: Specifies whether the service network filter displayed is active on this interface.

Instructions: Select Enable to enable the service network filter.

Select Disable to disable the service network filter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.2

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: None

Options: Any valid NetWare address in hexadecimal notation

Function: Specifies the network on which you want to apply the service network filter.

Instructions: Enter the address of the target network in hexadecimal format. Using a mask, you can make this stand for a single network or a range of networks with similar addresses. You can specify all networks by entering a Target Network of 0xFFFFFFFF and a Target Network Mask of 0xFFFFFFFF.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.6

Parameter: Target Network Mask (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: None

Options: Any valid IPX network address in hexadecimal notation

Function: The mask, combined with the Target Network parameter value, determines which networks will be filtered.

Instructions: Enter a network address or filter pattern of up to 8 hexadecimal characters. A mask of 0xFFFFFFFF specifies an exact match with the network address specified in the Target Network parameter. You can specify all networks by entering a Target Network of 0xFFFFFFFF and a Target Network Mask of 0xFFFFFFFF. A value of 0x0 is invalid.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.7

Parameter: **Target Service Type (hex)**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: None

Options: Any valid Novell server type number in 4-digit hexadecimal format

Function: Specifies the type of server that the filter should recognize in its criteria for allowing or disallowing certain SAP broadcasts to pass to the locally attached network segment.

Instructions: Enter the server type number in 4-digit hexadecimal format. Include leading zeros. For all types, enter a value of 0xFFFF. See Appendix D, "Common Service Types and Identifiers" for a list of valid server types.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.8

Parameter: **Filter Priority**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: None

Options: 0 to the number of filters of this type

Function: Specifies the priority of this filter in relation to other filters of the same type.

Instructions: Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.14

Parameter: **Mode**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: Outbound

Options: Outbound | Inbound | Both

Function: Specifies whether you want to apply the filter to inbound packets, outbound packets, or both.

Instructions: Specify Inbound if you want to apply the filter to SAP packets coming into this interface.

Specify Both if you want to filter both inbound and outbound packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.9

Parameter: Protocol

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: Any

Options: Any | Local | Static | SAP

Function: Applies this outbound filter only to services learned on the specified protocol when sending SAP updates. This does not apply to inbound services.

Instructions: Specify the protocol on which you want to apply the filter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.11

Parameter: Action

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: Advertise/Accept

Options: Advertise/Accept | Suppress

Function: Specifies how to process any SAP advertisement that matches the SAP filter criteria you established in the Target Network and Target Service Type parameters.

Instructions: Select Advertise/Accept to enable the filter to allow advertisement and acceptance of services that match the filter criteria you established in the Target Network and Target Service Type parameters.

Select Suppress to configure the IPX router to drop SAP advertisements that match the SAP filter criteria you established in the Target Network and Target Service Type parameters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.10

Parameter: Cost

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: 1 (for hop- or tick-based routing)

Options: 1 to maximum positive integer (if tick-based routing is enabled)

1 to one less than the value specified in the Maximum Hops parameter (if hop-based routing is enabled)

Function: Used only when the Action parameter is Advertise/Accept, this parameter assigns a cost for routes matching this filter. A zero cost indicates that the route's actual cost should be used. This parameter sets the cost (number of ticks or hops) for this interface. The cost is included in subsequent SAP packets sent to other interfaces. IPX drops the packet when its hop count exceeds a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network.

If the filter is an *inbound* filter, the entered cost replaces the cost associated with the server in SAP advertisements sent from this router.

If this is an *outbound* filter, the entered cost replaces the server's cost that is advertised in SAP packets by this router.

Instructions: Do not change the default value of this parameter unless you are an experienced IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value of this parameter can significantly affect router performance. If you are an experienced user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.12

IPX Service Name Filter Configuration Parameters

This section describes all parameters shown in the IPX Service Name Filter Configuration window (Figure B-21).

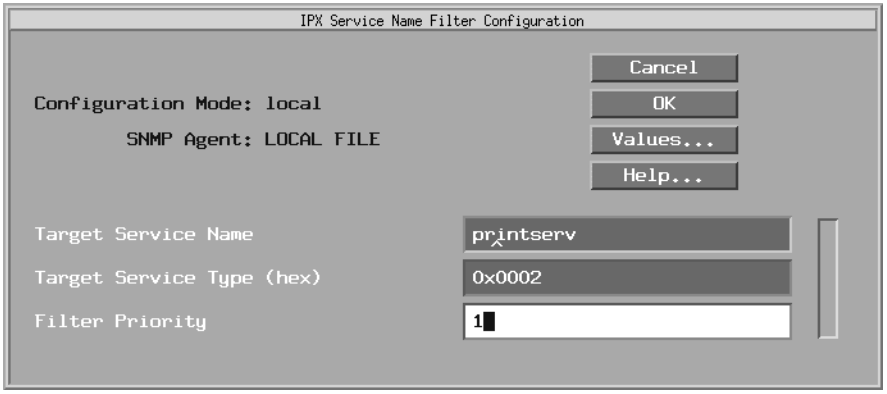

Figure B-21. IPX Service Name Filter Configuration Window

Parameter: Target Service Name

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Service Name Filters

Default: None

Options: Any valid alphanumeric service name or one containing wildcard characters or a pattern-matching regular expression

Function: This is the filter that you want to apply. It can specify the name of the server to which you are applying the service name filter, or it can be a filter containing a wildcard or a pattern (regular expression) to be matched. (See “Using Wildcards with SAP Filters” and “Using Pattern Matching with SAP Filters” for lists of these characters.)

Instructions: Enter a service name or filter pattern consisting of up to 48 alphanumeric characters, optionally including wildcards or a regular expression (pattern).

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.6

Parameter: **Target Service Type (hex)**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Service Name Filters

Default: None

Options: Any valid Novell service type number in 4-digit hexadecimal format

Function: Specifies the type of service that the filter should recognize in its criteria for allowing or suppressing certain SAP broadcasts to pass to the locally attached network segment.

Instructions: Enter the service type number in 4-digit hexadecimal format. Include leading zeros. For all types, enter a value of FFFF. See Appendix D, "Common Service Types and Identifiers" for a list of valid service types.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.7

Parameter: **Filter Priority**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Service Name Filters

Default: None

Options: 0 to the maximum number of filters of this type

Function: Specifies the priority of this filter in relation to other filters of the same type.

Instructions: Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.13

IPX Service Name Filter Parameters

This section describes how to set all parameters shown in the IPX Service Name Filters window (Figure B-22).

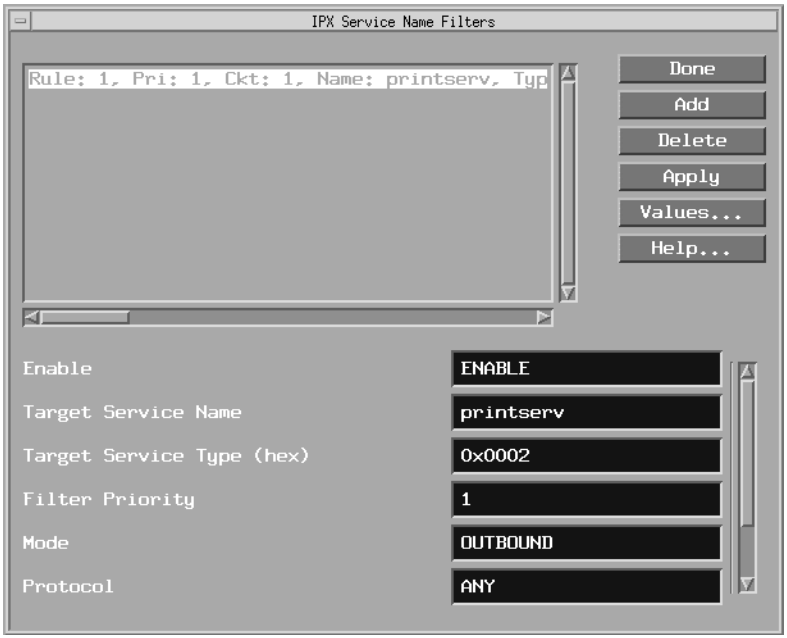

Figure B-22. IPX Service Name Filters Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter

Default: Enable

Options: Enable | Disable

Function: Specifies whether the service name filter displayed is active on this interface.

Instructions: Select Enable to enable the service name filter.

Select Disable to disable the service name filter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.2

Parameter: Target Service Name

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter

Default: None

Options: Any valid alphanumeric server name or one containing wildcard characters or a pattern-matching regular expression. (See “Using Wildcards with SAP Filters” and “Using Pattern Matching with SAP Filters” for lists of these characters.)

Function: This is the filter that you want to apply. It can specify the name of the server to which you are applying the server-level SAP filter, or it can be a filter containing a wildcard or a pattern (regular expression) to be matched.

Instructions: Enter a service name or filter pattern consisting of up to 48 alphanumeric characters, optionally including wildcards or a regular expression (pattern).

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.6

Parameter: Target Service Type (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter

Default: None

Options: Any valid Novell server type number in 4-digit hexadecimal format

Function: Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.

Instructions: Enter the server type number in 4-digit hexadecimal format. Include leading 0s. For all types, enter a value of 0xFFFF. See Appendix A for a list of valid service types.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.7

Parameter: Filter Priority

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter

Default: None

Options: 0 to the maximum positive integer

Function: Specifies the priority of this filter in relation to other filters of the same type.

Instructions: Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.13

Parameter: Mode

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter

Default: Outbound

Options: Outbound | Inbound | Both

Function: Specifies whether you want to apply the filter to inbound packets, outbound packets, or both.

Instructions: Accept the default, Outbound, if you want to apply the filter to SAP packets advertised by the specified interface.

Specify Inbound if you want to apply the filter to SAP packets coming into this interface. Specify Both if you want to filter both inbound and outbound packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.8

Parameter: Protocol

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter

Default: Any

Options: Any | Local | Static | SAP

Function: Applies this outbound filter only to services learned on the specified protocol when sending SAP updates. This does not apply to inbound services.

Instructions: Specify the protocol on which you want to apply the filter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.10

Parameter:	**Action**
Path:	Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter
Default:	Advertise/Accept
Options:	Advertise/Accept | Suppress
Function:	Specifies how to process any SAP advertisement that matches the SAP filter criteria you established in the Target Service Name and Target Service Type parameters.
Instructions:	Select Advertise/Accept to enable the filter to allow advertisement or acceptance of services that match the filter criteria you established in the Service Name and Service Type parameters. Select Suppress to configure the IPX router to drop SAP advertisements that match the SAP filter criteria you established in the Service Name and Service Type parameters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.9

Parameter:	**Cost**
Path:	Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter
Default:	1 (for hop- or tick-based routing)
Options:	1 to maximum positive integer (if tick-based routing is enabled) 1 to one less than the value specified in the Maximum Hops parameter (if hop-based routing is enabled)
Function:	Used only when the Action parameter is Advertise/Accept, this parameter assigns a cost for routes matching this filter. A zero cost indicates that the route's actual cost should be used. This parameter sets the cost (number of ticks or hops) for this interface. The cost is included in subsequent SAP packets sent to other interfaces. IPX disposes of the packet when its hop count passes a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Solutions Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router. If the filter is an *inbound* filter, the entered cost replaces the cost associated with the server in the SAP advertisement, and the router uses this cost in its calculations. If this is an *outbound* filter, the entered cost replaces the server's cost that is advertised in SAP packets by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.11

Appendix C
BCC show Commands for IPX

This appendix describes how to use the BCC show command to obtain IPX statistical data from the management information base (MIB). The type and amount of data displayed depend on the specific IPX settings you want to view. This appendix includes descriptions of the following show commands:

Topic	Page
show ipx summary	C-2
show ipx adjacent-hosts	C-2
show ipx forwards	C-3
show ipx hosts	C-3
show ipx interfaces	C-4
show ipx rips	C-5
show ipx route-filters	C-6
show ipx routes	C-7
show ipx saps	C-8
show ipx server-name-filters	C-8
show ipx server-network-filters	C-9
show ipx services	C-10
show ipx static-netbios-routes	C-11
show ipx static-routes	C-12
show ipx static-services	C-12
show ipx stats	C-13

show ipx summary

The **show ipx summary** command displays general information about IPX.

The output includes the following information:

Configured state	Specifies if IPX is configured on the router.
Current state	Specifies if IPX is enabled or disabled.
Multiple host address	Specifies if multiple host addressing is enabled.
Routing method	Identifies the routing method.
Maximum path	The maximum number of paths allowed.
Maximum path splits	Specifies if load balancing is enabled or disabled.
Log filter setting	The types of log messages that IPX filters.
Number of routes	The maximum number of destinations that the router will learn.
Number of services	The maximum number of routes the router will learn.
Number of hosts	The maximum number of next-hop hosts that the router will learn.
Number of IPX interfaces	The number of IPX interfaces configured.

show ipx adjacent-hosts

The **show ipx adjacent-hosts** command displays information for configured adjacent hosts.

The output includes the following information:

Interface Name	The name of the IPX interface.
Configured State	Specifies if IPX is configured on an adjacent host.
Current State	Specifies if IPX is enabled or disabled.
Host Address	The address of the adjacent host.

show ipx forwards

The **show ipx forwards** command displays IPX forwarding table information.

The output includes the following information:

Network	The network address.
Interface Name	The name of the IPX interface.
Type	The type of service.
Method	The routing method.
Equal-Cost-Path	The number of equal cost paths.

show ipx hosts

The **show ipx hosts** command displays IPX host table information.

The output includes the following information:

Host Address	The IPX host address.
Nexthop Interface	The address of the next-hop host.
Network	The network address.
Method	The encapsulation method.

show ipx interfaces

The **show ipx interfaces** command displays IPX interface configuration information.

The **show ipx interfaces** command supports the following command filters (flags) and filter arguments:

-encaps *<method>*	Displays information about an IPX interface with the specified encapsulation method.
-host *<address>*	Displays information about the IPX interface with the specified host address.
-net *<address>*	Displays information about the IPX interface with the specified network address.
-name *<symbolic_name>*	Displays information about the IPX host with the specified symbolic name.

The output includes the following information:

Interface Name	The name of the IPX interface.
Configured State	Specifies if IPX is configured on the router.
Current State	Specifies if IPX is enabled or disabled.
Network Address	The network address.
Host Address	The IPX host address.
Encapsulation Method	The encapsulation method used for this interface.

show ipx rips

The **show ipx rips** command displays IPX RIP interface record configuration information.

The output contains the following information:

Interface Name	Identifies the name of the IPX RIP interface.
Configured State	Specifies if IPX is configured on the router.
Current State	Specifies if IPX is enabled or disabled.
Update Interval	Specifies the frequency of RIP update packet transmissions.
Listen Mode	Specifies if this interface receives periodic or triggered updates.
Supply Mode	Specifies if this interface transmits periodic or triggered updates.
Packet In	Number of packets received.
Packet Out	Number of packets delivered.
Packet Bad	Number of packets corrupted.

show ipx route-filters

The **show ipx route-filters** command displays IPX route filter information.

The **show ipx route-filters** command supports the following command filters (flags) and filter arguments:

-direction *<filter_direction>*	Displays information about the IPX route filter that filters data packets travelling in the specified direction.
-net *<address>*	Displays information about IPX route filters applied to the specified network.
-proto *<protocol>*	Displays information about the IPX route filter applied to the specified protocol.
-action *<filter_action>*	Displays information about the IPX route filter that performs the specified action.
-interface *<name>*	Displays information about the IPX route filter applied to an interface having the specified symbolic name.

The output contains the following information:

Target Network	The network where the route filter is active.
Network Mask	The mask attached to the target network.
Current State	Specifies if the route filter is enabled or disabled.
Interface Name	Identifies the name of the IPX interface.
Priority	The priority of this filter in relation to other filters of the same type.
Action	Specifies how IPX processes any RIP advertisement that matches the route filter criteria.
Direction	Specifies whether the filter is applied to inbound packets, outbound packets, or both.

show ipx routes

The **show ipx routes** command displays IPX routing table information.

The **show ipx routes** command supports the following command filters (flags) and filter arguments:

-dest *<destination_network>*	Displays information about the the IPX route with the specified destination network.
-net *<address>*	Displays information about the IPX route with the specified network address.
-host *<address>*	Displays information about the IPX route having the specified host address.
-type *<destination_protocol>*	Displays information about the IPX route having the specified destination protocol.

The output contains the following information:

Dest Network	The target network.
Interface Name	The name of the IPX interface.
Nexthop Network	The address of the next-hop network.
Nexthop Host Address	The address of the next-hop host.
Type	The type of route.
Age	The granularity, in seconds, for aging RIP and SAP information.
Ticks	The cost, in ticks, for this interface.
Hops	The cost, in hops, for this interface.

show ipx saps

The **show ipx saps** command displays IPX SAP interface record configuration information.

The output contains the following information:

Interface Name	The name of the IPX SAP interface.
Configured State	Specifies if SAP is configured on the router.
Current State	Specifies if SAP is enabled or disabled.
Update Interval	Specifies the frequency of RIP update packet transmissions.
Listen Mode	Specifies if this interface receives periodic or triggered updates.
Supply Mode	Specifies if this interface transmits periodic or triggered updates.
Packet In	Number of packets received.
Packet Out	Number of packets delivered.
Packet Bad	Number of packets corrupted.

show ipx server-name-filters

The **show ipx server-name-filters** command displays IPX server name filter information.

The **show ipx server-name-filters** command supports the following command filters (flags) and filter arguments:

-direction *<filter_direction>*	Displays information about the IPX server name filter that filters data packets travelling in the specified direction.
-net *<address>*	Displays information about IPXserver name filter applied to the specified network.
-proto *<protocol>*	Displays information about the IPX server name filter applied to the specified protocol.
-interface *<name>*	Displays information about the IPX server name filter applied to and interface having the specified symbolic name.

The output contains the following information:

Server Name	The name of the server.
Server Network	The address of the server network.
Current State	Specifies if the server name filters feature is enabled or disabled.
Interface Name	The name of the IPX interface.
Prio	The priority of this filter in relation to other filters of the same type.
Filter Type	The type of filter.
Direction	Specifies whether the filter applies to inbound packets, outbound packets, or both.

show ipx server-network-filters

The **show ipx server-network-filters** command displays IPX server network filter information.

The **show ipx server-network-filters** command supports the following command filters (flags) and filter arguments:

-direction *<filter_direction>*	Displays information about the IPX server network filter that filters data packets travelling in the specified direction.
-net *<address>*	Displays information about IPX server network filter applied to the specified network.
-type *<protocol>*	Displays information about the IPX server network filter applied to the specified protocol.
-interface *<name>*	Displays information about the IPX server network filter applied to and interface having the specified symbolic name.

The output contains the following information:

Target Network	The network where the server network filter is active.
Network Mask	The mask attached to the target network.
Current State	Specifies if the service network filter is enabled or disabled.
Interface Name	Identifies the name of the IPX interface.
Prio	The priority of this filter in relation to other filters of the same type.
Filter Type	The type of filter.
Direction	Specifies whether the filter applies to inbound packets, outbound packets, or both.

show ipx services

The **show ipx services** command displays IPX services information.

The **show ipx services** command supports the following command filters (flags) and filter arguments:

-net *<address>*	Displays information about the IPX service having the specified network address.
-nexthophost *<host_address>*	Displays information about about the IPX service with a next-hop host that has specified network address.
-nexthopnet *<address>*	Displays information about the IPX service with a next-hop host that has address.
-type *<filter_type>*	Displays information about the IPX service having the specified filter type.

The output contains the following information:

Service Name Hops	The cost, in hops, for routes matching this filter.
Interface Name	The name of the IPX interface.
Type	The Novell service type.
NextHop Network	The address of the next-hop network.
NextHop Host Address	The address of the next-hop host.
Network	The address of the network.
Age	The granularity, in seconds, for aging RIP and SAP information.

show ipx static-netbios-routes

The **show ipx static-netbios-routes** command displays IPX NetBIOS static route information.

The **show ipx static-netbios-routes** command supports the following command filters (flags) and filter arguments:

-net *<target_net_address>*	Displays information about the IPX NetBIOS static route having the specified target network address.
-name *<target_name>*	Displays information about the IPX NetBIOS static route having the specified symbolic target name.

The output contains the following information:

Target Name	The name of the target server.
Target Network	The address of the target network.
Current State	Specifies if the static NetBIOS routes feature is enabled.

show ipx static-routes

The **show ipx static-routes** command displays IPX static route information.

The **show ipx static-routes** command supports the following command filters (flags) and filter arguments:

-net *<address>*	Displays information about the IPX static route having the specified network address.
-nexthophost *<host_address>*	Displays information about the IPX static route with a next-hop host that has the specified address.
-nexthopnet *<net_address>*	Displays information the IPX static route with a next-hop host that has the specified network address.

The output contains the following information:

Static Network	The address of the static network.
State	The state of the NetBIOS static route.
Interface Name	The name of the IPX interface.
NextHop Network	The address of the next-hop network.
NextHop Host Address	The address of the next-hop host.
Ticks	The cost, in ticks, for this interface.
Hops	The cost, in hops, for this interface.

show ipx static-services

The **show ipx static-services** command displays IPX static service table information.

The output contains the following information:

Serv. Name	The symbolic name of the server.
Network	The network address.
Host Address	The host address.
Hops	The cost, in hops, for this interface.
Interface Name	Identifies the name of the IPX interface.
Nexthop Network	The address of the next-hop network.
Type	The type of service.
Sock	The socket address of this service.

show ipx stats

The **show ipx stats** command displays IPX statistical information.

The output contains the following information:

Name	The name of the IPX interface.
Network	The network address.
In Receive	Number of packets received.
In Deliver	Number of packets delivered.
Out Request	Number of packet requests.
Forward	Number of packets forwarded.
In Discard	Number of packets received that were discarded.
Out Discard	Number of packets sent that were discarded.

Appendix D
Common Service Types and Identifiers

Table D-1. Service Types and Identifiers

Service Type	Hexadecimal Identifier
Wildcard	FFFF
Unknown	0000
User	0001
User Group	0002
Print Queue	0003
NetWare File Server V3.*x*	0004
Job Server	0005
Gateway	0006
Print Server	0007
Archive Queue	0008
Archive Server	0009
Job Queue	000A
Administration	000B
Diagnostics	0017
NetBIOS	0020
NAS SNA Gateway	0021

(continued)

Table D-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
NACS	0023
Remote Bridge Server	0024
Bridge Server	0026
TCP/IP Gateway (Racal-Datacom)	0027
Eicon X.25 Point-to-Point GW	0028
Eicon 3270 Gateway	0029
(CHI) Corp	002A
Unknown	002C
Time Synchronization Server	002D
Archive Srvr Dynamic SAP/SMS TSA	002E
DI3270 Gateway	0045
Advertising Print Server	0047
TCP/IP Gateway (Racal-Datacom)	0048
Unknown	004A
Btrieve VAP 5.*x*	004B
NetWare SQL VAP/NLM	004C
Xtree Network Version	004D
Btrieve VAP 4.*x*	0050
QuickLink (Cubix)	0052
Print Queue User	0053
ARCserve VAP	0055
Eicon X.25 Multi-Point Gateway	0058
ARCserv	0064
ARCserve 3.0	0066

(continued)

Table D-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
WANcopy Utility	0072
Cheyenne ARCserv 5.0 Intel	0077
TES-NetWare for VMS	007A
Emerald Backup/WATCOM Debugger	0092
TES-NetWare for VMS	0095
NetWare Access Server (NAS)	0098
SQL Server (Named Pipes)	009A
NetWare Access Server	009B
Portable NetWare/SunLink NVT	009E
Progress Database Server	009F
PowerChute APC UPS NLM	00A1
Compaq IDA Status Monitor	00AC
Unknown	0100
Intel LAN Protect Bindery	0102
Oracle Database Server	0103
NetWare 386, Remote Console	0107
Novell SNA Gateway	010F
HP Print Server	0112
CSA MUX	0114
CSA LCA	0115
CSA CM	0116
CSA SMA	0117
CSA DBA	0118
CSA NMA	0119

(continued)

Table D-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
CSA SSA	011A
CSA STATUS	011B
CSA APPC	011E
SNA TEST (SAA profile)	0126
CSA TRACE	012A
Unknown	012E
Communications Executive	0130
NFS Domain Server	0133
NetWare Naming Service (NNS) Profile	0135
NNS Queue/NW Print Queue	0137
NNS Domain Scheme Descriptor	0138
Intel LANSpool VAP	0141
Aladdin Knowledge	0142
Optical Drives	0143
IrmaLAN Gateway	0152
Named Pipe Server	0154
Intel PICKIT/CAS Talk Server	0168
Unknown (User)	0173
Compaq SNMP Agent	0174
Xtree Server	0180
Xtree	0189
NetWare Access Server	018A
GARP Gateway (Net Research)	01B0
BindView (LAN Support Group)	01B1

(continued)

Table D-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
Intel LanDesk Manager	01BF
Unknown	01CA
Shiva Netmodem	01CB
LanRover	01CC
Castelle FAXPress Server	01D8
Castelle LANPress Print Server	01DA
Unknown	01E4
Legato	01F0
Legato	01F1
SQL Server	0200
NMA Agent (NMS; socket 0x2F90)	0233
LANZ Agent (Socket 0x401F; NetExp)	0237
LANZ Agent (Socket 0x4800)	0238
NMS Hub Management	0239
LANZ Agent (Socket 0x401F)	023A
NetWare SMS (Storage Management System)	023F
NetWare Connect	024E
NMS Console (name-stnMAC+IPX#)	026A
NW4 Time Sync Server (Socket 0x040)	026B
NW4 NDS Server	0278
NetWare for SAA Gateway	0304
Gallacticom BBS	030A
HP LaserJet (Quick Silver)	030C
Attachmate 3270 Gateway	0320

(continued)

Table D-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
Multi Server Director	0327
Intel NetPort II	0361
ECS Cheyenne ARCserv 5.0 Intel	0375
Cheyenne ARC Serv 5.0 Intel SE	0376
PowerChute Version 3.0 (new)	037E
ViruSafe Notify	037F
HP Bridge	0386
HP Hub	0387
NetWare SAA Gateway	0394
Lotus Notes (OS/2 version)	039B
Central Point Anti Virus NLM	03B7
ARCserve 4.0 (socket 0x 8600)	03C4
Intel LANSpool 3.5	03C7
Lexmark 4033 Print Server	03D5
NetWare SQL/Gupta NLM	03DE
UNIXWare	03E1
UNIXWare	03E4
NetWare File Server Version 4.*x*	0400
NetSprint print server	0414
SiteLock Virus	0429
ARCserve 5.0	044C
Dell SCSI Array (SDA) Monitor	045B
Sybase	0474
Sybase	0475

(continued)

Table D-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
Novix TCP/IP support NLM	04DC
SiteLock Checks	0520
Certus Anti Virus NLM (master)	0523
SiteLock Checks	0529
Delrina WinFax Pro network	0553
McAfee's NetShield anti-virus	0580
SiteLock	0B29
SiteLock Applications	0C29
SofTrack for NW Version 3.*x*	0C2C
LAI SiteLock	2380
Meeting Maker	238C
SofTrack for NW Version 4.*x*	2C0C
SiteLock Server (Brightworks)	4808
SiteLock User	5555
Tapeware	6312
Rabbit 3270 Gateway	6F00
Intel NetPort (Print Server)	8002
WordPerfect Network Version	8008
Unknown	8069
Unknown	8746
McAfee's NetShield anti-virus	9000
SQL Monitor (IPX)	9604
Unknown	9892
Unknown	C00C

(continued)

Table D-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
SiteLock Metering VAP/NLM	F11F
SiteLock	F1FF
SQL Server (IPX)	F503

Appendix E
Sample IPX Configuration

This appendix provides a sample IPX configuration. Depending on the interface type and service requirements, the network uses different encapsulations. Configurations are provided for Router 1 and Router 2 (Figure D-1). The network configuration lists Router A and Router B but does not provide configurations for them.

The following assumptions apply:

- The router uses the tick-based RIP method.
- The frame relay cloud is non-fully meshed and all PVCs are group mode. You have set the management type to default.
- You have configured RIP for all interfaces.
- You have enabled Multiple Host Addressing under IPX Global.
- Default settings are in effect for all timer values.

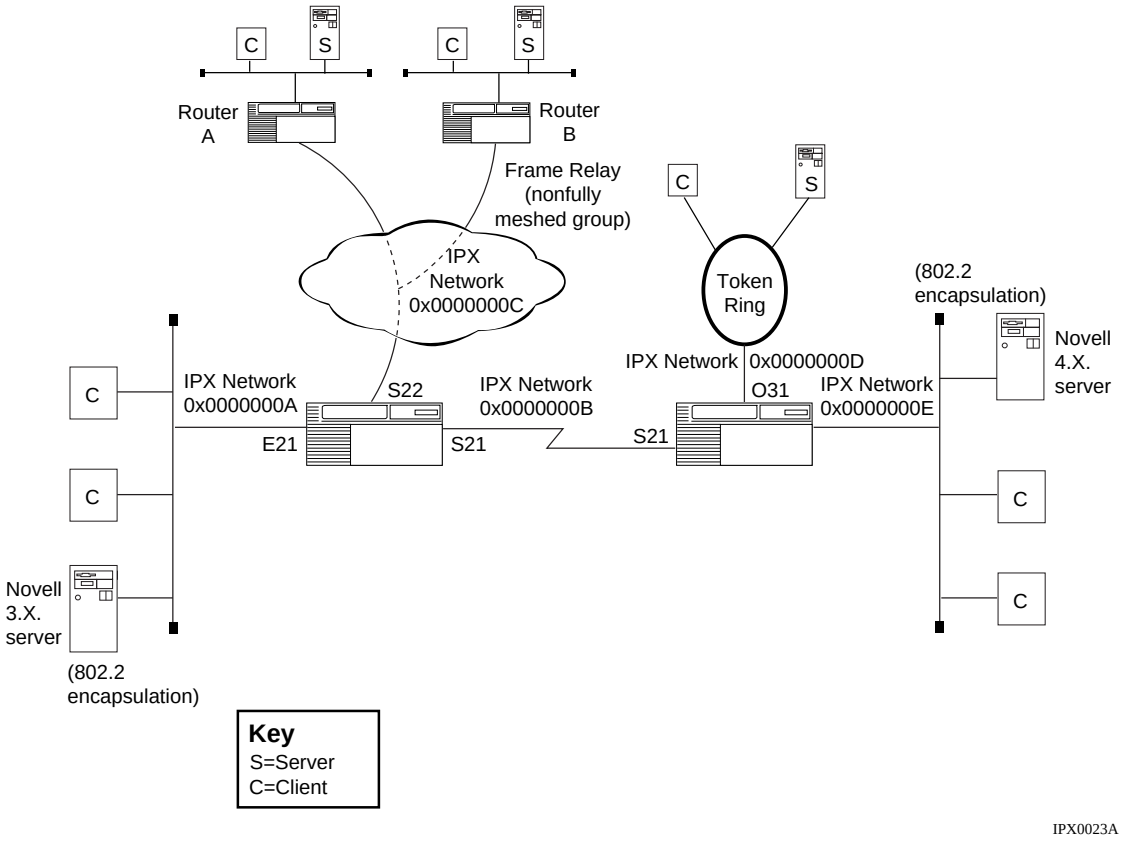

Figure E-1. Sample IPX Configuration

Configuration Particulars

Router 1

Edit the E21 circuit and add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000A and the Configured Encaps parameter to Novell.

Edit the S21 circuit and set the WAN protocol to Standard. Add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000B.

Edit the S22 circuit and set the WAN protocol to Frame Relay. Add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000C and click on OK. Select Protocols > IPX > Interfaces, and highlight the IPX Network parameter, which should be set to 0x0000000C. Click on the RIP button and set the Split Horizon parameter to Disable.

Note: Turn off Split Horizon on the frame relay hub router if the spoke routers are to learn routes from each other. However, leave Split Horizon enabled on spoke routers.

Router 2

Edit the E21 circuit and add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000E.

Edit the S21 circuit and set the WAN protocol to Standard. Add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000B.

Edit the 031 circuit and set the ring speed to 16 MB. Add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000D and the Configured Encaps parameter to SNAP.

Index

A

accessing IPX parameters
  using the Technician Interface, B-9
acronyms, xix
action
  SAP filters, 6-123
adding
  IPX route filters, B-67
  RIP to an interface, 3-4
  service network filter, B-74
adjacent host, 1-3
  configuration parameter descriptions, B-50
  parameter descriptions, B-53
advanced global parameters
  descriptions, B-22
  editing, B-22
advertisement interval (RIP), 6-43
Age Multiplier
  IPX RIP circuit parameter, B-37
  IPX SAP circuit parameter, B-43
Aging Frequency
  advanced global parameter, B-18
Aging Pending Frequency
  advanced global parameter, B-19
ATM
  circuits, 6-39

B

bandwidth, 6-110, 6-111
bandwidth-on-demand, 6-101
bindery
  and SAP, 6-56
bridge
  source route bridge end station support, 6-26
broadcast filter
  NetBIOS, 6-88

C

change circuit parameters
  editing, B-40
characters in SAP pattern matching filters, 6-129
circuits
  LAN and WAN, 1-17
client/server connection
  example, 1-15
  role of Bay Networks router, 1-13
concatenation rules and operators
  SAP pattern matching filters, 6-131
configurable RIP timers, 6-43
configurable SAP timers, 6-58
configurable split horizon, 6-49
Configured Encaps
  IPX interface parameter, B-26
configuring
  RIP and SAP broadcast timers, 6-109
  service network filter parameters, 6-133, B-74
configuring IPX
  on a token ring interface, 4-6
connection negotiation
  IPXCP, 5-13
  IPXWAN, 5-13
connectionless datagram protocol, 1-2
conventions, text, xviii

Cost
IPX interface parameter, B-25
tick, 6-38

D

data link layer addresses, 1-6, 4-5
datagram, 1-2
default route
support, 1-3
deleting
IPX route filters, B-74
RIP from an interface, 3-5
service name filters, B-88
static routes, B-61
static services, B-67
deleting a service network filter, B-82
Destination Count
advanced global parameter, B-17
dial backup, 6-101
dial services
advantages of, 6-101
descriptions, 6-101
types of, 6-101
Dial-on-Demand, 1-3, 6-102
with static routing, 6-103, 6-111
with traffic filters, 6-104
dynamic routing, 1-3

E

editing
IPX change circuit parameters, B-40
IPX interface parameters, B-22
route filter configuration parameters, B-67
server name filter parameters, 6-134, A-21
static route parameters, B-59
static routes, B-56
static service parameters, B-64
editing IPX advanced global parameters, B-22
educational services, xxii
Enable
IPX interface parameter, B-23
encapsulation method, 4-2
encapsulation types. *See* frame encapsulation types
end station support, 1-5
end station support token ring
end station support, 6-26

F

filter
adding service network filters, B-74
deleting service name filters, B-88
editing service name filters, 6-134, A-21
NetBIOS broadcast, 6-88
SAP, 6-122
SAP filter concatenation rules and operators, 6-131
SAP filter pattern matching, 6-123
SAP filtering example, 6-133
SAP filters prohibiting SAP broadcasts, 6-73
SAP filters with pattern matching, 6-129
SAP pattern matching characters, 6-129
service name filter configuration parameters, B-82
service network filter parameters, 6-133, B-74, B-77
traffic filters with dial-on-demand, 6-104
filters
SAP filters with wildcards, 6-127
frame encapsulation types, 4-1, 4-11
frame formats, 1-17
frame relay, 5-2, 5-3
circuits, 6-39
fully meshed network, 6-50
split horizon enabled, 6-50

G

global parameters
advanced, descriptions, B-22
advanced, editing, B-22

H

HDLC encapsulation, 6-35
hop
as basis for routing decision, 1-5
definition, B-14
RIP maximum, 6-17

hop count, B-14
host
  Router Host Number parameter, B-11
Host Count
  advanced global parameter, B-18
host ID numbers
  on a token ring circuit, 4-6
Host Number
  adjacent host parameter, B-51
  IPX interface parameter, B-25

I

Immediate Update
  IPX SAP circuit parameter, B-46
information broadcast
  RIP, 6-39
interface parameters
  editing, B-22
Internet Data Packet (IDP) format, 1-2
internetwork addressing, 1-2
intranode addressing, 1-2
IP
  starting, 3-2, 3-3
IP Address parameter
  IP configuration, 3-3
IPX
  background information, 1-17
IPX advanced global parameters
  descriptions, B-22
  editing, B-22
IPX change circuit parameters, B-40
IPX interface parameters
  editing, B-22
IPX over WAN media, 1-3
  link configurations, 5-14
IPX parameters
  accessing via Technician Interface, B-9
IPX ping, 1-5
IPX ping support, 1-13
IPX route filter parameters
  descriptions, B-69
IPX service name filter
  configuration parameter descriptions, B-82
  parameter descriptions, B-84
IPX service network filter parameters
  descriptions, B-77
IPX static service
  configuration parameter descriptions, B-61
  parameter descriptions, B-64
IPX watchdog acknowledgment, 6-104
IPX Watchdog Spoofing
  IPX interface parameter, B-29
IPXCP, 1-3, 5-2
  link configurations, 5-14
  link negotiation, 5-13
  sample configuration, 5-12
  using, 5-2
IPXWAN, 1-3, 5-2
  link configurations, 5-14
  link negotiation, 5-13
  sample configuration, 5-12
  using, 5-2
IPXWAN connection
  negotiating, 5-3

L

LAN
  circuits, 1-17
  logical, 4-2
  physical, 4-2
link delay
  WAN link, 5-3
link negotiation, 5-2
  IPXCP, 5-13
  IPXWAN, 5-13
load redistribution and rerouting, 1-10
load sharing, 1-5, 1-7, 1-10
Local IPX watchdog acknowledgment, 6-104
Log Filter
  advanced global parameter, B-15
logical LAN, 4-2
logical network address, 4-2

M

Maximum Hops
advanced global parameter, B-16
Maximum Path
advanced global parameter, B-15
IPX advanced global parameter, 6-15
Maximum Path Splits
advanced global parameter, B-16
Multicast Address
IPX interface parameter, B-28
multiline, 1-12
multiline circuits, 1-10
differences from multipath, 1-11
multipath configurations, 1-10
multipath routing, 1-5, 1-7, B-16
precedence/priority, 1-10
multiple circuits per segment, 1-12
multiple interfaces per circuit, 1-12
multiple IPX interfaces per circuit, 1-3
multiple-host router, 1-12, 4-7

N

Name
IPX interface parameter, B-23
NCP (Network Control Protocol), 5-3
NDS (NetWare Directory Services), 6-58
Nearest Server Reply
IPX SAP circuit parameter, B-44
negotiation
IPXCP link, 5-13
IPXWAN connection, 5-3
IPXWAN link, 5-13
NetBIOS
broadcast packet (Type 20), 6-82
Type 20 broadcast packets, 1-5
NetBIOS Accept
IPX interface parameter, B-27
NetBIOS broadcast filtering, 6-88
NetBIOS Deliver
IPX interface parameter, B-27
NetBIOS packet
filtering, 6-91
use with nonstandard static routing, 6-86
use with standard static routing, 6-88
NetBIOS packet flow, 6-92
NetBIOS static routes
configuration parameter descriptions, B-46
parameter descriptions, B-48
NetWare
bindery, 6-56
Directory Services (NDS), 6-58
Novell, 4-3
network
fully meshed, 6-50
nonfully meshed, 6-50
network address
logical, 4-2
Network Control Protocol (NCP), 5-3
network number, 5-3
primary, 5-6
network-level services, 1-3
nonfully meshed network, 6-50
split horizon disabled, 6-51
Novell
NetWare, 4-3
standards, 6-110
Novell Certification Conformance
advanced global parameter, B-21
Novell, Inc., 1-2
number of IPX interfaces per circuit, 4-11

P

Pace
IPX RIP circuit parameter, B-37
IPX SAP circuit parameter, B-42
Packet Size
IPX RIP circuit parameter, B-38
IPX SAP circuit parameter, B-44
pattern matching
concatenation rules and operators, 6-131
SAP filters, 6-123, 6-129
periodic RIP advertisement interval, 6-43, 6-58

Permanent Virtual Circuit (PVC), 5-3
physical LAN, 4-2
ping, 1-13
ping capability, 1-5
PNN (primary network number), 5-6
PPP (point-to-point protocol), 5-2, 5-3
precedence/priority
  multipath routing, 1-10
Primary Net Number
  IPX global parameter, B-22
primary network number (PNN), 5-6
product support, xxii
publications
  Bay Networks, xxi
purging
  RIP entries, 6-43
PVC (Permanent Virtual Circuit), 5-3

R

regular expression (RE), 6-129
request packet (RIP), 6-38
response packet (RIP), 6-38
RFC
  IPX source documents, 1-17
RFC 1552, 1-17, 5-2
RFC 1634, 1-17, 5-2
RIF (Routing Information Field), 6-27
RIP, 1-5, 6-38
  adding to an interface, 3-4
  deleting from an interface, 3-5
  starting, 3-4
RIP (Routing Information Protocol), 1-3
  maximum timer ticks, 6-17
  update packet transmissions frequency, 6-109
RIP broadcast timers
  configuring, 6-109
RIP information broadcast, 6-39
RIP request packet, 6-38
RIP response packet, 6-38
RIP timers
  configurable, 6-43
route filter configuration parameters
  editing, B-67
route filters
  adding, B-67
  deleting, B-74
  dropping all routes, 6-119
  parameter descriptions, B-69
router
  multiple-host, 1-12, 4-7
  single-host, 1-12, 4-9
Router Host Number
  IPX global parameter, B-11
router information broadcast, 6-39
Router Name
  IPX global parameter, B-7, B-11
router name
  valid characters in, 5-9
routes
  dropping all, 6-119
Routing Information Field (RIF), 6-27
Routing Information Protocol (RIP), 1-3, 1-5, 6-38
routing table, 6-38, 6-39
running IPX
  over frame relay, 5-3
  over PPP and frame relay, 5-3

S

SAP, 1-5
  and NDS, 6-58
  and the NetWare bindery, 6-56
SAP (Service Advertising Protocol), 1-3
SAP broadcast timers
  configuring, 6-109
SAP filters, 6-131
  example, 6-133
  pattern matching, 6-123, 6-129
  pattern matching characters, 6-129
  prohibiting SAP broadcasts, 6-73
  service network configuration parameters, B-74
  wildcards and pattern matching, 6-127

SAP service
configuration parameters, B-61
deleting, B-67
SAP timer
configurable, 6-58
SAP update packet transmissions frequency, 6-109
server name filter parameters
editing, 6-134, A-21
Service Advertising Protocol (SAP), 1-3, 1-5
Service Count
advanced global parameter, B-17
service name filters
configuration parameter descriptions, B-82
deleting, B-88
parameter descriptions, B-84
service network filter
adding, B-74
configuration parameter descriptions, B-74
service network filter parameters
configuring, 6-133, B-74
descriptions, B-77
service network filters
dropping all services, 6-133
service types, D-1
services
dropping all, 6-133
show commands
command syntax, C-2
online Help for, C-2
wildcard search characters, C-2
Single Route Explorer (SRE) frame, 6-27
single-host router, 1-12, 4-9
SMDS
circuits, 6-39
socket
numbers, 1-2
source route bridge end station support, 6-26
source routing, 1-5
split horizon, 1-5
configuring, 6-49
disabled in a nonfully meshed network, 6-51
enabled in a fully meshed network, 6-50
SRE frame, 6-27
standard IPX configurations
multiple-host router, 4-7
single-host router, 4-9
starting
IP, 3-2, 3-3
RIP, 3-4
static routes
configuration parameter descriptions, B-56
deleting, B-61
NetBIOS configuration parameters, B-46
nonstandard NetBIOS use, 6-86
parameter descriptions, B-59
parameter editing, B-59
support, 1-3
using, B-56
with Dial-on-Demand, 6-103
with standard NetBIOS routing, 6-88
static service configuration parameters
descriptions, B-61
static service parameters
editing, B-64
static services
deleting, B-67
parameter descriptions, B-64
SAP service network configuration, 6-72
support, Bay Networks, xxii

T

Target Network
IPX NetBIOS static route parameter, B-47, B-49
Target Server
IPX NetBIOS static route parameter, B-47
technical publications, xxi
technical support, xxii
Technician Interface
accessing IPX parameters, B-9
text conventions, xviii
tick
as basis for routing decision, 1-5
cost, 6-38
definition, 6-38, B-14
RIP timer maximum, 6-17
tick-based routing, 5-3

timeout
RIP entries, 6-43
timer
configurable SAP timers, 6-58
RIP (configurable), 6-43
RIP and SAP broadcast, 6-109
token ring
configuring host ID numbers, 4-6
token ring interface
configuring IPX on, 4-6
TR End Station
IPX interface parameter, B-26
traffic filters
with Dial-on-Demand, 6-104
Type 20 broadcast packet
NetBIOS, 1-5, 6-82

U

Unnumbered RIP, 1-3
Update Interval
IPX RIP circuit parameter, B-37
IPX SAP circuit parameter, B-43
upper-layer protocol
handling packets associated with, 1-5

W

WAN
circuits, 1-17
link delay, 5-3
media, 5-2
watchdog acknowledgment, 6-104
Watchdog Spoofing parameter (IPX), B-29
wildcard search characters, used with show commands, C-2
wildcards
with SAP filters, 6-127

X

Xerox Network System (XNS), 1-2